Insurance as a Risk Management Instrument for Energy Infrastructure Security and Resilience

U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Infrastructure Security and Energy Restoration

This page intentionally left blank.

Preface

This study examines key risks that the Nation's critical energy infrastructure is confronting and the ways in which the insurance industry can help manage these risks, including how it identifies, assesses, and manages them and their potential impacts. Today, weather-related incidents account for the majority of economic losses in the insurance industry as well as in the critical infrastructure sectors. In addition to the traditionally-recognized natural hazards, critical energy infrastructure faces significant emerging threats, including cybersecurity and space weather risks.

While the United States has a large, mature insurance market, developing insurance mechanisms for protecting critical infrastructure from these emerging risks remains a significant challenge. The lack of historical data on the frequency and severity of these events, the changing nature of technologies impacted by them, as well as the inherent uncertainties posed by these risks make it difficult to accurately assess these emerging risks and develop proper insurance products. Insurance instruments can be a useful risk mitigation tool for critical infrastructure by encouraging resilience-enhancing investments and facilitating recovery after a disaster. However, due to the increased interdependencies across various critical infrastructure systems and sectors as well as the growing dependence of today's society on the critical infrastructure functions and advanced technologies, the question of insurability of critical infrastructure against emerging risks faces new challenges.

For Further Information

This report was prepared by the Office of Electricity Delivery and Energy Reliability under the direction of Patricia Hoffman, Assistant Secretary, and William Bryan, Deputy Assistant Secretary.

Specific questions about information in this report may be directed to Dr. Kenneth Friedman, Senior Policy Advisor (kenneth.friedman@hq.doe.gov).

Tiffany Y. Choi of ICF International contributed to this report.

The U.S. Department of Energy would like to acknowledge the following reviewers for their contribution to this report:
Ebert, Michael, Volgenau School of Engineering, George Mason University
Hartford Steam Boiler (A member of the Munich Reinsurance Company)
Klingman, Charles
Munich Reinsurance Group
National Association of Insurance Commissioners
Prof. Michel-Kerjan, Erwann, The Wharton School, University of Pennsylvania
Reinsurance Association of America
Zurich Insurance Group Ltd.

Cover photo sources:
High-voltage transmission lines: Florida Department of Environmental Protection
Aerial views showing the damage caused by Hurricane Sandy: Reuters/Mark C. Olsen/U.S. Air Force/Handout
Solar flares: Huffingtonpost.com
Cybersecurity threats: kam.lt

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

Executive Summary

In this report, the Office of Electricity Delivery and Energy Reliability (OE), U.S. Department of Energy (DOE) examined key risks that critical energy infrastructure is confronting and the ways in which the insurance industry can help manage these risks. In most developed countries, including the United States, insurance is one of the principal risk management instruments, not only for aiding in recovery after a disaster, but also for encouraging future investments that are more resilient to potential hazards. Therefore, this study examined how the insurance industry perceives and manages risks, including identification and assessment of risks, as well as the methodologies to quantify and measure their potential impacts.

Today, weather-related incidents account for the majority of economic losses in the insurance industry, and they pose a significant threat to the Energy Sector.[1] With the abundance of historical data on natural disasters and their economic impacts, the insurance industry has developed and maintained technical and actuarial expertise for providing risk assessment and risk allocation mechanisms. According to the insurance industry, economic losses—both insured and uninsured—resulting from natural hazards in the United States have been on the rise and are expected to continue to grow in the future. However, despite the mature and large insurance market—$1.7 trillion or a third of the world's insurance market—no universal or standardized methodology exists in the United States to measure or quantify the impacts of natural hazards.

In addition to the increasing variability of and costs resulting from weather-related events, the Energy Sector is facing new, emerging threats, including cybersecurity and space weather risks. Cybersecurity risk is seen as a rapidly growing and evolving threat against critical infrastructure, including that of the Energy Sector. On the other hand, while space weather risk is not completely new—scientists know the possible causes and effects of solar events from previous cycles—the economic impacts that could result from solar weather events are far less certain.

Due to the increasing dependency on advanced technology and the growing interdependency of the global economy, the number and types of infrastructure and systems that can be affected by these emerging risks have increased considerably. While there are a growing number of sources that attempt to measure or quantify the threats and consequences of emerging risks, currently-available data are inadequate to accurately assess these risks or develop proper insurance products.

To be insurable, an event must be predictable in frequency and severity (i.e., assessable), so that an appropriate premium that corresponds to the underlying risk can be determined (i.e., economically viable) and a large number of affected parties can share and diversify the risk (i.e., mutual). However, due to the lack of historical data, inherent uncertainties posed by some of the phenomena, as well as the changing nature of technologies that are impacted by emerging risks such as cybersecurity and space weather, neither frequency nor severity can be assessed to calculate an appropriate premium that is mutual or economically viable. In addition, both of

[1] The Energy Sector, as delineated by the Homeland Security Presidential Directive 7, includes the production, refining, storage, and distribution of oil, gas, and electric power, except for hydroelectric and commercial nuclear power facilities..

these emerging risks may not meet the "randomness" requirement (i.e., the occurrence of event is unpredictable or random) of insurability, because cyber attacks are usually planned ahead and carefully targeted in highly-concentrated geographical areas or in certain industries (i.e., power plants), whereas the timing and geographical location of solar storms can be predicted albeit without great accuracy.

Other challenges in developing insurance instruments for emerging risks include:

- The general public's low level of familiarity with emerging risks;
- The fluctuation of risks and threats driven by technology advancement as well as changing mitigation, restoration, and recovery approaches;
- The risk of a regional, national, or global catastrophic event, resulting in an overwhelming number and cost of claims;
- Lack of adequate reinsurance or government intervention as the "insurer of last resort";
- The misconception by the insured that existing insurance products or self-insurance are sufficient to cover emerging risks; and
- The price volatility of insurance products due to the evolving nature of threats and the uncertainty in the potential effects of such risks.

While insurance instruments can be a useful financial risk mitigation tool for critical infrastructure, they also face a variety of complex challenges. The public sector's engagement may be necessary to develop and maintain certain insurance programs; however, the respective roles and responsibilities of public and private partners in providing adequate protection for critical infrastructure against emerging risks through insurance remain unclear.

I. Introduction

In this report, the Office of Electricity Delivery and Energy Reliability (OE), U.S. Department of Energy (DOE) examined a variety of risks that the Nation's critical energy infrastructure is confronting and the ways in which the insurance industry[2] can help manage these risks. Energy infrastructure and systems are large, fixed assets with long lifetimes, and man-made and natural hazards can cause a serious harm to the infrastructure and result in a considerable economic damage. Although natural disasters traditionally have been a key focus of the Energy Sector's[3] efforts, the sector has also been considering serious, emerging threats such as cybersecurity and space weather risks, including the possible impacts of electromagnetic pulse. Therefore, this report examined how the insurance industry perceives and manages risks, including the identification and assessment of risk characteristics, as well as the methodologies to quantify and measure the risks' potential impacts.

1.1 Background and Purpose of the Study

Within DOE, OE is the lead office supporting the Federal government's recovery and restoration efforts responding to energy emergencies, particularly through the U.S. Department of Homeland Security (DHS)'s Federal Emergency Management Agency (FEMA) Emergency Support Function (ESF) #12—Energy.[4] Per the Energy Sector-Specific Plan, DOE supports the Energy Sector's activities to enhance energy infrastructure resilience against all hazards, which is an "ongoing effort that will require continued vigilance, contingency planning, and training."[5]

The Presidential Policy Directive 8 (PPD-8), released in March 2011, mandated the National Preparedness Goals and System, which describes the Nation's approach to preparing for the threats and hazards that pose the greatest risk to the security of the United States.[6] Specifically, PPD-8 identified five mission areas—prevention, protection, mitigation, response, and recovery—to achieve the goal of a secure and resilient Nation. One of the core mission areas, mitigation,[7] refers to the efforts to improve the resilience of critical infrastructure, to reduce vulnerabilities from all hazards, and to lower future risks after a disaster has occurred. Insurance can be one of such mitigation instruments for infrastructure resilience, as it can induce investments to lessen the impacts of disasters affecting critical infrastructure. Also, insurance is a crucial recovery[8] tool that provides financial support necessary to facilitate recovery, ensuring social and economic continuity in the aftermath of a disaster.

---

[2] The terms "insurance" and "reinsurance" are delineated in Section 1.2; however, both words are used synonymously to describe an industry throughout the report unless otherwise noted.

[3] The Energy Sector, as delineated by the Homeland Security Presidential Directive 7 (HSPD-7), includes the production, refining, storage, and distribution of oil, gas, and electric power, except for hydroelectric and commercial nuclear power facilities. The Energy Sector is not monolithic and contains many interrelated industries that support the exploration, production, transportation, and delivery of fuels and electricity to the U.S. economy.

[4] The U.S. Department of Energy (DOE), Emergency Support Function #12 – Energy Annex, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf (accessed November 1, 2012).

[5] The Energy Sector Specific Plan, DOE and the U.S. Department of Homeland Security (DHS), 2010, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_2010.pdf (accessed June 29, 2012).

[6] DHS, Presidential Policy Directive / PPD-8: National Preparedness, March 11, 2011, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm (accessed June 29, 2012).

[7] In the PPD-8, "mitigation" is defined as the "capabilities to reduce loss of life and property by lessening the impact of disasters."

[8] In the PPD-8, "recovery" refers to the "capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and

In most developed countries, insurance is one of the principal mechanisms used by individuals and organizations for managing risk, not only for aiding in recovery after a disaster but also for encouraging future investments that are more resilient to potential hazards. Today, weather-related incidents account for the majority of economic loss in the insurance industry, and they are also a significant threat to the energy infrastructure. According to the insurance industry, damages resulting from natural hazards in the United States have been on the rise and are expected to continue to grow in the future. In addition to the increasing variability of weather-related events, the Energy Sector is facing new, emerging threats, including cybersecurity and space weather risks.

This study examined the insurance industry's perspectives on the various natural and man-made hazards, including: (1) the definition of key terms such as natural disaster, catastrophe, and emerging risks; (2) the role of insurance in risk management of critical infrastructure; (3) global historical trend of weather events and their impacts; (4) the relationship between climate variability and energy infrastructure; and (5) selected emerging risks in the Energy Sector, including cybersecurity and space weather events. While insurance can play an important role in encouraging investments that enhance resilience and in facilitating recovery after a disaster, it also faces complex challenges in providing adequate risk management strategies, particularly concerning emerging risks affecting critical energy infrastructure.

1.2 Insurance and Risk Management

Insurance has become an increasingly important part of developed economies, as a financial mechanism for individuals and organizations—including critical infrastructure owners and operators—to manage risks. A risk, as defined by the insurance industry, consists of three components—hazard, vulnerability, and exposure—all of which can change over time.[9] Many critical infrastructure risks are covered by the insurance industry, providing financial compensation mechanisms against selected risks. Risk management is not about removing all risk, but about operating at an acceptable or optimal level of risk; hence, through insurance, owners and operators can choose to manage risks in three ways—accepting, mitigating, or transferring them.[10]

> "In addition to its prime role in recovery, insurance can be a powerful tool in inducing critical infrastructure investments that enhance prevention and response."
>
> - *The Challenge of Protecting Critical Infrastructure,* The Wharton School of the University of Pennsylvania, October 2005

Accepting risk, often practiced through self-insurance, is optimal when the costs of mitigation and risk transfer are too high relative to the perceived probability and magnitude of loss. In self-insurance, asset owners and operators set aside funds to specifically cover the costs of potential damage. Large energy infrastructure owners and operators often choose this option if the cost of purchasing third party insurance is too costly, the

long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources."

[9] Eichner, J., "Space Weather Risks from an Insurance perspective," Munich Re, April 26, 2011, http://www.swpc.noaa.gov/sww/sww11/SWW_2011_Presentations/SWW_Boulder_MunichRE_EICHNER.pdf (accessed October 31, 2012).

[10] "Insurance and Critical Infrastructure Protection: Is there a Connection in an Environment of Terrorism?" Canadian Centre of Intelligence and Security Studies, The Norman Paterson School of International Affairs Carleton University, March 2006, http://www3.carleton.ca/cciss/res_docs/ceip/rowlands_devlin.pdf (accessed July 6, 2012).

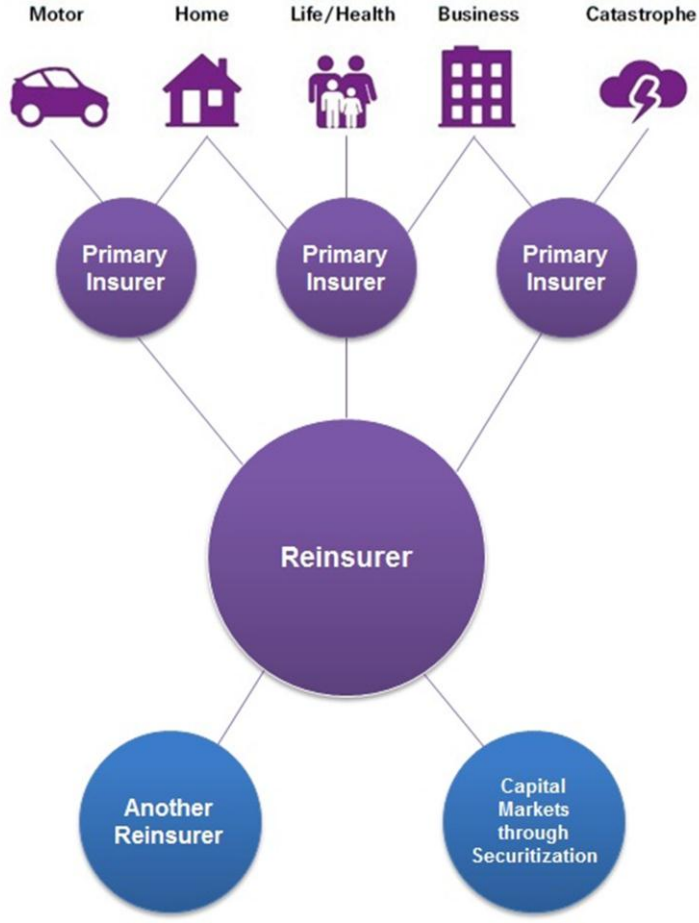
perceived risk is small, or the risk is so new that it is not well understood.

Improved risk mitigation, through integrative risk management approaches, can reduce losses. However, risk mitigation through prevention, the hardening of assets, and effective remediation, may involve investments that are costly. While new facilities may be able to integrate innovations that can mitigate risk more effectively, it is not always financially sensible to retrofit older facilities.

Risk transfer generally means third party insurance. While no universal definition of insurance exists, most definitions of insurance contain two key elements—risk transferring and risk sharing.[11] Insurance is a mechanism for sharing or spreading risks over time and over a large group and geographical areas. This allows for the financial disaster consequences that occur to be shared by a large group of people, rather than the burden falling only on the affected individuals or communities.[12]

The second element of insurance, risk transfer, is typically provided in insurance coverage that transfers an uncertain and possibly large loss into a certain, small cost or premium for the insured. Often, the risks are transferred once again from an insurer to another entity called a reinsurer. As illustrated in Figure 1, risks are transferred from individuals and companies, and then through primary insurers to reinsurers. In essence, reinsurance is insurance for insurance companies.[13]

Figure 1. Risk Transfers in Insurance and Reinsurance



Source: Swiss Re, 2010.

In short, insurance provides a method to distribute and reduce the financial risk associated with adverse events, by sharing costs either among individuals or over time, enabling the insured to balance their available funds over time and with various parts of the

[11] GAO, Definitions of Insurance and Related Information, GAO-06-424R, February 23, 2006, http://www.gao.gov/assets/100/94044.pdf (accessed June 29, 2012).
[12] Federal Emergency Management Agency (FEMA), Training Course, "Comparative Emergency Management, Session 16: Risk Transfer, Sharing, and Spreading."
[13] "The essential guide to reinsurance," Swiss Re, 2010. http://media.swissre.com/documents/The_Essential_Guide_to_Reinsurance_EN.pdf (accessed July 5, 2012).

world.[14] Any quantifiable or estimated risk can potentially be insured, and there are a wide variety of insurance products available to individuals and business as illustrated in Figure 1.

While insurance is a form of financial risk management, this technically does not reduce actual disaster consequences or reduce hazard likelihood.[15] But because of their experience in identifying, analyzing, and modeling risks, insurance and reinsurance companies may be able to help existing and potential customers better understand the possible risks they face and help them develop and implement enhanced risk management strategies and practices.

The discussion of insurance in this report is on its roles and capabilities as a risk management instrument. Further information about the insurance industry's structure, business model, productivity, or products can be found in the various references provided in the bibliography of this report. The next section of the report discusses some of the key terms used to describe hazards and risks, followed by the historical trends and impacts of catastrophes worldwide assessed by the insurance industry.

II. Key Terms and Definitions

Each year, hundreds of weather-related events occur throughout the world, ranging from high winds, drought, and storms to hurricanes and earthquakes. Most of these events, however, do not result in significant economic cost or loss of life; in fact, only a fraction of these events cause monetary damage or are considered a natural disaster or catastrophe. In discussing and assessing risk management efforts, it is important to understand some of these key terms, such as natural hazard, natural disaster, and catastrophe, notwithstanding these events are often multifaceted and open to a range of different interpretations. This section discusses a variety of commonly-used terms for describing adverse events in the United States.

> "Natural hazards in of themselves—hurricanes, floods, droughts—are not disasters. Rather it is their consequences and the ability of the local community to respond to them that determine whether the event is characterized as a disaster."
>
> - *The Year that Shook the Rich,* The Brookings Institution, March 2012

Natural disaster. For the purpose of this study, natural disaster carries the meaning as defined in the Robert T. Stafford Disaster Relief and Emergency Assistance Act, which means "any hurricane, tornado, storm, flood, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, drought, fire, or other catastrophe in any part of the United States which causes, or which may cause, substantial damage or injury to civilian property or persons."[16] In other words, natural hazards alone do not always constitute a disaster; rather, the degree to which the natural hazard creates negative consequences determines whether an event is a disaster.

[14] "Extreme events and insurance: 2011 annus horribilis," The Geneva Association, March 2012, http://www.genevaassociation.org/PDF/Geneva_Reports/GA-2012-Geneva_report%5B5%5D.pdf (accessed July 5, 2012).
[15] FEMA Training Course, "Comparative Emergency Management: Session 16: Risk Transfer, Sharing, and Spreading."
[16] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 U.S.C. 5121-5207, and Related Authorities, http://www.fema.gov/pdf/about/stafford_act.pdf (accessed May 31, 2012).

Major disaster. In the United States, an adverse event becomes a "major disaster" when the President determines that the severity and magnitude of the damages caused by the event are beyond the combined capabilities of State and local governments to respond and warrant Federal disaster assistance.[17] The major disaster declaration by the President enables the Federal government to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby. Note, however, the parameters for defining a "substantial damage" are unclear. Similarly, a catastrophe is described without specific parameters as follows.

Catastrophe. For the U.S. government, the term "catastrophic incident" means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area.[18]

In contrast with these abstract definitions used by the U.S. government, the insurance industry applies a set of quantitative parameters to define the same terms. According to the definition set by the Insurance Services Office Property Claims Services Division (ISO PCS), a primary source of insured loss evaluation used by the U.S. insurance industry, an event is designated as a catastrophe in the United States when it affects a significant number of policyholders and insurers as well as causes insured property damage of $25 million or more.[19] Note, however, that this does not appear to be a universal definition as further explained in the next section.

2.1 Catastrophe Classifications Used by the Insurance Industry

No single definition of disaster exists in the world. Various sources identify and assess a wide range of hazards, both natural and man-made. One way to assess an event is through quantification of loss in terms of human life and monetary value, as done by the insurance industry. While the definitions of disaster provided by the U.S. government are abstract, the insurance industry applies a set of specific criteria to define, categorize, and quantify disasters and catastrophes. This section compares the criteria for defining a catastrophe developed by two of the world's largest reinsurance companies—Munich Reinsurance Company (Munich Re) and Swiss Reinsurance Company Ltd. (Swiss Re).[20] In addition to these criteria and definitions,

[17] FEMA, Disaster Declaration Process, http://www.fema.gov/media/fact_sheets/declaration_process.shtm (accessed June 1, 2012).
[18] The Homeland Security Act of 2002, Public Law 109-295, as amended, 6 U.S.C. 311-321j, http://uscode.house.gov/pdf/2006/2006usc06.pdf (accessed June 25, 2012).
[19] "PCS Catastrophe Serial Numbers," Insurance Services Office Property Claims Services Division (ISO PCS), http://www.iso.com/Products/Property-Claim-Services/PCS-Catastrophe-Serial-Numbers.html (accessed January 30, 2013). ISO PCS is the primary insurance-industry resource for compiling and reporting estimates of insured property losses resulting from catastrophes in the United States. See http://www.isopropertyresources.com/Products/Property-Claims-Service/Property-Claim-Services-PCS.html (accessed January 31, 2013).
[20] For additional sources on the various definitions of catastrophe, see "Chapter 17 Annex - OECD: Review of the Main Initiatives on Collection and Dissemination of Cat Risk Exposures and Losses" of *Improving the Assessment of Disaster Risks to Strengthen Financial Resilience: A Special Joint G20 Publication by the Government of Mexico and the World Bank*, by the Organisation for Economic Co-operation and Development (OECD), June 2012, http://www.gfdrr.org/sites/gfdrr.org/files/GFDRR_G20_Low_June13.pdf (accessed February 7, 2013).

extensive historical catastrophe data developed by these two reinsurance firms are referenced and analyzed throughout this paper.

Figure 2 is a set of criteria that Swiss Re used for determining catastrophic events in 2011.[21] Swiss Re defined a catastrophe in two broad categories—natural and man-made—as follows:

- **Natural catastrophe:** Refers to an event caused by natural forces . . . the scale of losses resulting from a catastrophe depends not only on the severity of the natural forces concerned, but also on man-made factors, such as building design or the efficiency of disaster control in the afflicted region.
- **Man-made disaster:** Refers to major events associated with human activities or "man-made" or "technical" disasters. The following categories exist in man-made disasters: major fires and explosions, aviation and space disasters, shipping disasters, rail disasters, mining accidents, collapse of buildings/bridges, and miscellaneous (including terrorism).[22]

Figure 2. Swiss Re's Criteria for Catastrophic Events in 2011

		Threshold in USDm
Insured losses (claims):	Maritime disasters	18.0
	Aviation	35.9
	Other losses	44.6
or Total economic losses:		89.2
or Casualties:	Lost or missing lives	20
	Injured	50
	Homeless	2 000

Source: Swiss Re Sigma Report, February 2012.

An event is included in Swiss Re's database if insured claims, the total economic losses, or the number of casualties exceed a certain threshold set in these criteria, which is annually adjusted for inflation. According to Swiss Re's criteria seen in Figure 2, an event that resulted in more than $89.2 million or more than 20 casualties was considered a catastrophic event in 2011.

Table 1 lists the categories of loss events developed and used by Munich Re's NatCatSERVICE—one of the most comprehensive databases available on natural catastrophe losses.[23] Unlike Swiss Re's database, Munich Re's database identifies and analyzes only natural events. Depending on the financial and human impact, events are assigned to one of six loss categories—from a pure natural event without any loss (category 0) to a great natural catastrophe (category 6).[24] Munich Re assesses both insured and overall losses, and the term "insured losses" covers all losses sustained by the insurance industry in all property insurance classes, except liability losses.

According to these criteria, the threshold for a catastrophe rose from an overall loss of $25 million in the 1980s to $60 million in 2010. Today, a natural event becomes a major catastrophe

[21] "Natural catastrophes and man-made disasters in 2011: historic losses surface from record earthquakes and floods," Sigma, Swiss Re, February 2012, http://media.swissre.com/documents/sigma2_2012_en.pdf (accessed July 9, 2012).
[22] Ibid.
[23] Munich Re NatCatSERVICE, http://www.munichre.com/en/reinsurance/business/non-life/georisks/natcatservice/default.aspx (accessed June 26, 2012).
[24] Munich Re, Loss database for natural catastrophes worldwide, http://www.munichre.com/app_pages/www/@res/pdf/natcatservice/database/catastrophe_classes_touch_en.pdf (accessed July 6, 2012).

if greater than a $250 million overall loss or more than 100 fatalities occur. A great natural catastrophe or a "great disaster" is defined more abstractly, mirroring the definition established by the United Nations, which describes a disaster as "a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources."[25]

Table 1. Catastrophe Categories Used by Munich Re

Catastrophe category		Overall losses					and/or fatalities
		Loss profile	1980s*	1990s*	2000s*	2010*	
0	Natural event	No property damage	-	-	-	-	none
1	Small-scale loss event	Small-scale property damage	-	-	-	-	1-9
2	Moderate loss event	Moderate property and structural damage	-	-	-	-	>10
3	Severe catastrophe	Severe property infrastructure and structural damage	US$ >25m	US$ >40m	US$ >50m	US$ >60m	>20
4	Major catastrophe	Major property, infrastructure and structural damage	US$ >90m	US$ >160m	US$ >200m	US$ >250m	>100
5	Devastating catastrophe	Devastating losses within the affected region	US$ >275m	US$ >400m	US$ >500m	US$ >650m	>500
6	Great natural catastrophe „GREAT disaster"	Region's ability to help itself clearly overtaxed, interregional/international assistance necessary, thousands of fatalities and/or hundreds of thousands homeless, substantial economic losses (UN definition). Insured losses reach exceptional orders of magnitude.					

*Losses adjusted to the decade average.

Source: Munich Re, 2011.

In addition to commonly-known hazards, the insurance industry also identifies and studies new, potential risks or "faint, initial signals" that may or may not further develop into real threats, often referred to as "emerging risks."[26]

Emerging risk, in the insurance industry, is loosely defined as a developing or changing risk which is difficult to assess or quantify.[27] It is a challenge to identify and analyze emerging risks, in large part due to their inherent characteristics—high uncertainty about the frequency and severity of the event, which make it challenging to quantify or communicate about the risks and consequences. Insurance firms investigate these risks because of their potential impact on their business and their clients. Thus the goal of the insurance business is to translate risks associated

[25] United Nation Office for Disaster Reduction (UNISDR), 2009 UNISDR Terminology on Disaster Risk Reduction, http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf (accessed June 26, 2012).
[26] "Spotlight on emerging risks," Swiss Re, http://www.swissre.com/rethinking/emerging_risks/QA_Reto_Schneider.html (accessed October 1, 2012).
[27] Ibid.; "Emerging Risks," Lloyd's, http://www.lloyds.com/The-Market/Tools-and-Resources/Research/Exposure-Management/Emerging-risks (accessed June 25, 2012).

with high uncertainty into quantifiable risks in order for insurance companies to offer products to customers to help them manage the real or perceived risks.

Global re/insurance firms and other financial institutions, individually as well as collaboratively, identify and assess emerging risks because they have a potential to affect their business. For example, re/insurance companies such as Munich Re, Swiss Re, Allianz, and Lloyd's each have designated specific resources to focus on emerging risks, as do other global organizations. For example, the World Economic Forum,[28] an international organization providing an independent, impartial assessment of global risks, conducts an annual survey with more than hundreds of experts and industry leaders worldwide to identify new global risks. Commercial Risk Europe[29]—a pan-European newspaper dedicated to news, trends, and issues critical to corporate risk and insurance management executives across Europe—also develops an annual publication to gauge the state of the European risk and insurance management community, including emerging risks. Finally, the Chief Risk Officer's (CRO) Forum,[30] represented by chief risk officers of large multi-national insurance companies, provides insights on emerging and long-term risks.

In the next section, the historical trend of catastrophes worldwide is discussed, followed by a discussion of selected emerging risks—cybersecurity and space weather risks—affecting the Energy Sector.

III. Insurance Industry Assessment of Historical Catastrophes

Currently, no standardized method for assessing disaster impact exists in the world. As the National Academy of Sciences (NAS)'s 1999 study found, no widely-accepted, consistent system or framework existed for assessing the economic impact and losses of natural disasters.[31] Thus, an important weakness with current disaster data is the lack of standardized methodologies and definitions. Recognizing the variances in the disaster data collected by the insurance industry, this section explores the global historical trend of catastrophes. The assessment in this section is based on the data developed and annually published by the world's two largest reinsurance firms,[32] Munich Re and Swiss Re, as well as the Insurance Information Institute and the ISO PCS.[33]

3.1 Global Historical Trend of Natural Disasters

The world has seen increasing losses—both insured and uninsured—resulting from catastrophic events since the mid-1980s. While this trend has been widely observed, the numbers of events

[28] World Economic Forum, http://www.weforum.org/ (accessed October 2, 2012).
[29] Commercial Risk Europe, http://www.commercialriskeurope.com/ (accessed October 17, 2012).
[30] The CRO Forum, http://www.thecroforum.org/about.html (accessed October 2, 2012).
[31] "The Impacts of Natural Disasters: A Framework for Loss Estimation," National Academy of Sciences, Washington, D.C., 1999.
[32] For a list of top 25 reinsurance groups ranked in by net written premiums in 2009, see http://pdf.computing.co.uk/REI_07-0810.pdf?id=0 (accessed October 2, 2012).
[33] For additional disaster loss databases, see "Chapter 17 Annex - OECD: Review of the Main Initiatives on Collection and Dissemination of Cat Risk Exposures and Losses" of *Improving the Assessment of Disaster Risks to Strengthen Financial Resilience: A Special Joint G20 Publication by the Government of Mexico and the World Bank,* by the Organisation for Economic Co-operation and Development (OECD), June 2012, http://www.gfdrr.org/sites/gfdrr.org/files/GFDRR_G20_Low_June13.pdf (accessed February 7, 2013).

recorded by different organizations vary significantly. For example, Munich Re's NatCatSERVICE holds more than 30,000 entries of historical data with some 1,000 entries being recorded each year; Swiss Re holds more than 7,000 entries and enters approximately 300 loss events per year.[34] The differences in the number of events recorded may be attributed to the fact that Swiss Re Sigma[35] uses the event (which may affect multiple countries) as the basis for each entry while Munich Re's data contains individual entries for each country affected, as well as the different criteria used by each firm for characterizing a disaster or catastrophic event as illustrated in Figure 2 and Table 1.[36]

In 2011, Swiss Re recorded a total of 325 catastrophic events, including both man-made and natural disasters, whereas Munich Re entered 820 natural disasters.[37] Nonetheless, both firms reported climbing insured losses, largely driven by the increased occurrences and insured economic impacts of natural catastrophic events. Between 1981 and 2011, natural disasters, including earthquakes, caused approximately 80 percent of insured losses in the world, whereas man-made disasters were blamed for 20 percent.[38] In addition, Swiss Re identified more than a $254 billion gap between the total economic loss and the insured loss in 2011, suggesting that a lack of insurance coverage continues to leave many individuals, companies, and governments financially vulnerable to catastrophic incidents.[39]

Assessing the overall impact of loss events is a challenge because what is considered in the total or overall loss evaluation varies by organization. For example, Swiss Re defines "total losses" as all the financial losses directly attributable to a major event such as damage to buildings, infrastructure, and vehicles, including losses due to business interruption as a direct consequence of the property damage. Total loss figures, however, do not include indirect financial losses—i.e. loss of earnings by suppliers due to disabled businesses, estimated shortfalls in gross domestic product, and non-economic losses, such as loss of reputation or impaired quality of life.[40] In contrast, Munich Re's assessment of economic losses includes direct losses of tangible goods, as well as separate information on indirect economic losses—losses resulting from the physical destruction of assets— where reliable information is available.[41]

In 2007, to better assess natural disaster impacts, Munich Re and Swiss Re, together with the United Nations Development Programme, the Asian Disaster Reduction Centre, and the

[34] Much Re NatCatSERVICE, http://www.munichre.com/en/reinsurance/business/non-life/georisks/natcatservice/default.aspx (accessed August 29, 2012).
[35] Swiss Re Sigma reports offer in-depth analysis of economic trends and strategic issues in insurance, reinsurance and financial services, covering life and non-life business. See http://www.swissre.com/sigma/ (accessed August 22, 2012).
[36] Ibid.
[37] Swiss Re Sigma, February 2012; Munich Re, Press Release, January 4, 2012, http://www.munichre.com/en/media_relations/press_releases/2012/2012_01_04_press_release.aspx (accessed June 22, 2012).
[38] Swiss Re Sigma, Insured catastrophe losses, 1970-2011, http://www.swissre.com/sigma/ (accessed August 22, 2012).
[39] Swiss Re Sigma, February 2012.
[40] *Improving the Assessment of Disaster Risks to Strengthen Financial Resilience: A Special Joint G20 Publication by the Government of Mexico and the World Bank*, by the Organisation for Economic Co-operation and Development (OECD), June 2012.
[41] Ibid.

International Strategy for Disaster Reduction, defined a common set of terminologies and the hierarchy of natural hazards. As provided in Table 2, natural hazards are categorized into four main hazard groups—geophysical, meteorological, hydrological, and climatological—and under each hazard category are the corresponding main and sub events.

Table 2. Hierarchy and Terminology of Natural Hazards

Hazard Group	Main Event	Sub-event
Geophysical	Earthquake	Earthquake Fire Tsunami
	Volcanic eruption	Volcanic eruption
	Mass movement dry	Subsidence Rockfall Landslide
Meteorological	Storms	Tropical storm (hurricanes, typhoon, cyclone)
		Extratropical storm (winter storm, blizzard / snow storm)
		Convective storm (severe storm, thunderstorm, lightning, hailstorm, tornado)
		Local storm (orographic storm)
Hydrological	Flood	General flood Flash flood Storm surge Glacial lake outburst flood
	Mass movement wet	Subsidence Avalanche Landslide
Climatological	Extreme temperature	Heat wave Cold wave / frost Extreme winter conditions
	Drought	Drought
	Widfire	Forest fire, bush fire, brush fire, grassland fire

Note: Munich Re's Geo Risks Research Group is responsible for screening of all aspects in the field of natural hazards and disasters, including geophysical hazards, weather-related hazards and potential consequences of climate change—in particular impacts of novel hazards and hazards that emerge from changes in vulnerability (such as space weather). However, space weather events, which can impact satellites, telecommunications, navigation systems, and the electric grid, have not been defined or included as part of the natural hazards.

Source: © 2011 Münchener Rückversicherungs-Gesellschaft, Geo Risks Research, NatCatSERVICE.

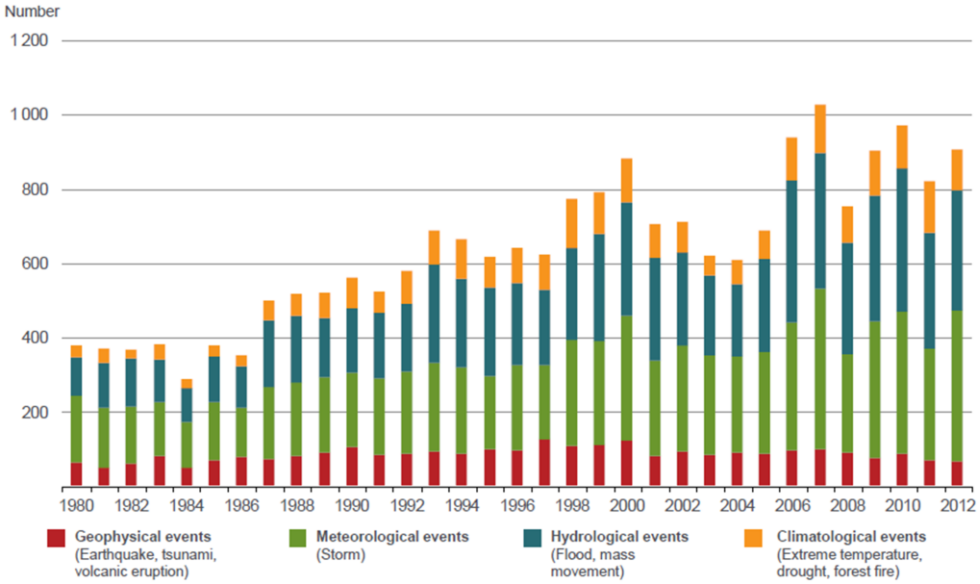
Globally, 2011 was the most expensive year in history in terms of insured natural disaster losses. According to Munich Re, 820 weather and climate disasters were documented around the world in 2011 that resulted in an estimated 27,000 deaths and $380 billion in total economic losses.[42] Of the total economic loss in 2011, $275 billion were uninsured, leaving approximately 72 percent of the affected without financial recovery mechanism through insurance. Damages resulting from the earthquake and tsunami in Japan in March accounted for more than half of the total loss, with approximately $210 billion in monetary damages and more than 15,840 fatalities.[43] The previous record for highest economic loss was $262 billion in 2005, the year in which hurricanes Katrina and Rita struck the Gulf of Mexico. (See Figures 3 and 4 by Munich

[42] Munich Re NatCarSERVICE, 2012.
[43] Rice, D. "2011 was costliest year in world disasters," USA Today, January 4, 2012, http://www.usatoday.com/weather/news/extremes/story/2012-01-04/world-disasters-costliest-earthquake-tsunami/52377642/1 (accessed June 22, 2012).

Re [the figures are adjusted for inflation]). Figure 3 is an assessment of global historical trend of weather events and Figure 4 shows the overall economic losses—insured and uninsured—caused by these events between 1980 and 2012.[44]

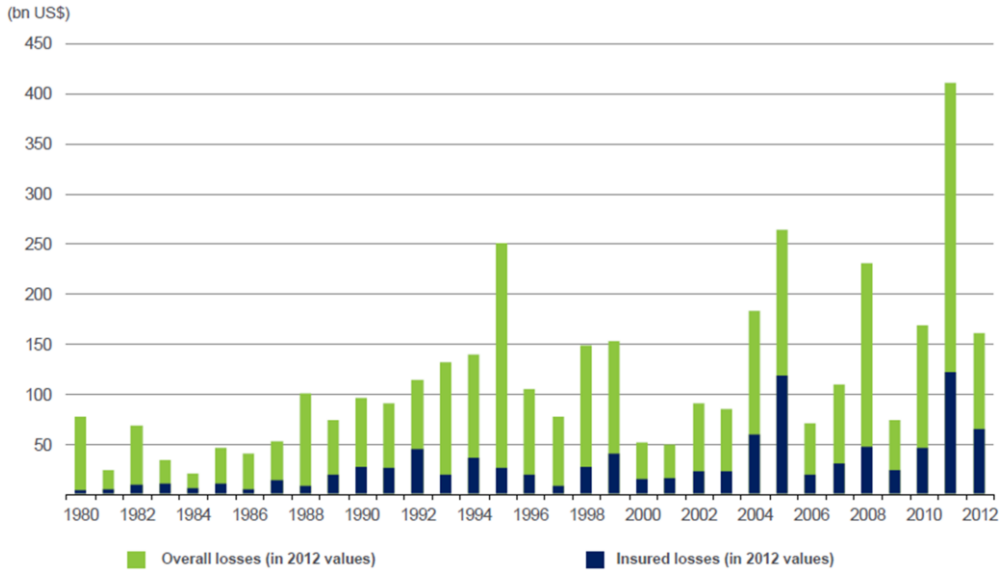
Munich Re's database records hundreds of loss events each year, which, depending on financial and human impact, are assigned to one of six loss categories—from a small scale loss event to a

Figure 3. Munich Re's Assessment of Natural Catastrophes Worldwide From 1980 to 2012



Source: Munich Re NatCatSERVICE, 2013.

Figure 4. Munich Re's Assessment of Losses From Natural Catastrophes Worldwide From 1980 to 2012



Source: Munich Re NatCatSERVICE, 2013.

[44] Munich Re Press Release, January 4, 2012, http://www.munichre.com/en/media_relations/press_releases/2012/2012_01_04_press_release.aspx (accessed June 22, 2012).

great natural catastrophe (see Table 1 in Section 2.1). This evaluation and its statistics do not consider pure natural events (catastrophe category 0) that do not result in a loss.

As illustrated in Figure 4, both insured and uninsured losses have been on the rise, although the overall losses were significantly lower in 2012 than in the previous year. In 2012, natural catastrophes caused $160 billion in overall losses and $65 billion in insured losses worldwide. Of the total economic loss, approximately 67 percent of overall losses and 90 percent of insured losses were attributable to the United States in 2012—compared to the respective historical averages of 32 percent and 57 percent—due to weather-related natural catastrophes including Hurricane Sandy (see Section 3.2 for discussion on natural disaster trends in the United States).

Historically, meteorological events have caused the most significant economic damages, accounting for approximately 77 percent of the total insured loss caused by "devastating"[45] or "great" disasters in the last 30 years or $600 billion.[46] (See Appendix B for Munich Re's assessment of "great and devastating" natural catastrophes in the world between 1980 and 2010. Also see Appendix C for Swiss Re's assessment of historical catastrophic events worldwide, including man-made events such as the September 11, 2002 terrorist attack.)

Although it is uncertain whether natural disasters are occurring more often than before, it is clear that the economic cost as a result of them is rising. According to various analyses, this is because a growing share of the world's population and economic activity is being concentrated in disaster-prone places—on tropical coasts and river deltas, near forests and along earthquake fault lines.[47] Other reasons for increasing cost of natural disasters include population growth, better standards of living, concentration of people and economies in large metropolises, susceptibility of modern societies and technologies to natural hazards, increasing insurance density,[48] and changes in environmental conditions.[49]

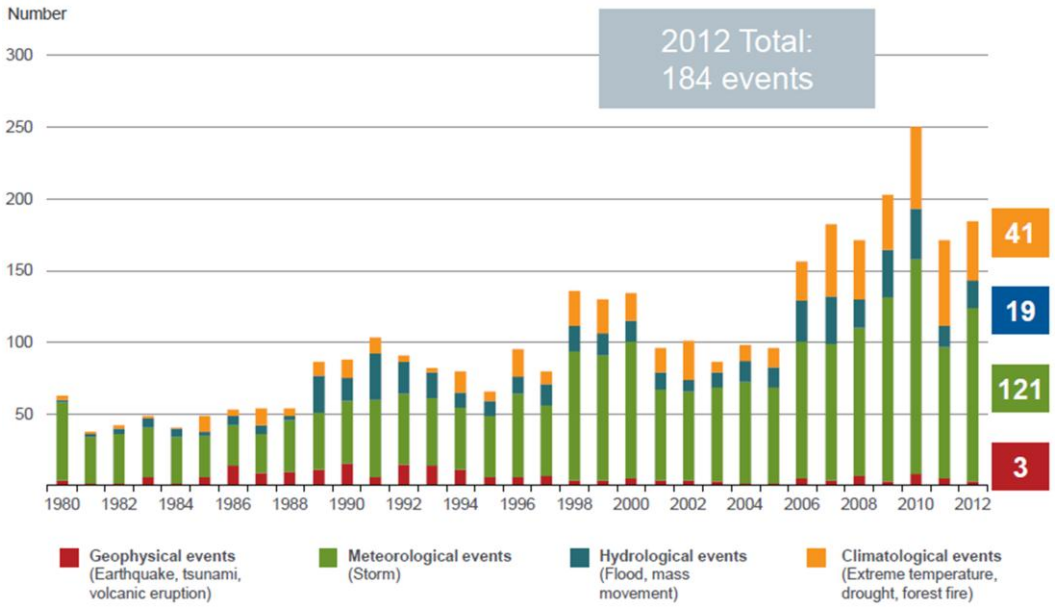
3.2 Natural Disaster Trends in the United States

The global trend of rising natural disaster losses has also been observed in the United States. Figure 5 is a historical trend of natural disasters in the United States between 1980 and 2012, and Figure 6 is the total economic losses—both insured and uninsured—caused by these events during the same period. In 2012, approximately 184 natural disasters occurred in the United States, and almost two thirds, or 121 events, were meteorological events. Climatological events—including extreme temperature, drought, and forest fire—have been occurring more

[45] An event is classified as a "devastating catastrophe" if the number of fatalities exceeds 500 and/or the overall loss exceeds $650 million. See Table 1.
[46] "TOPICS GEO, Natural catastrophes 2010: Analyses, assessments, positions," Munich Re, 2011, www.munichre.com/publications/302-07225_en.pdf (accessed November 20, 2012).
[47] "Natural disasters: Counting the cost of calamities," The Economist, January 14, 2012, http://www.economist.com/node/21542755 (accessed July 18, 2012).
[48] The term "insurance density" is used as a key indicator of the state of development of an insurance market. Insurance density indicates how much each inhabitant of a country spends each year for insurance services. See http://vig.online-report.eu/2007/ar/companiesmarketandstrategy/centralandeasterneurope/insurancedensity.html (accessed October 2, 2012).
[49] Hoeppe, P., "Worldwide Natural Disasters-Effects and Trends," Munich Re, http://www.munichre-foundation.org/NR/rdonlyres/E7ED6B1D-2D9F-4E64-9FB3-5C8A4539AD9B/0/20051116_Hoeppe_Hohenkammer_short_WEB.pdf (accessed July 18, 2012).

frequently and accounted for 22 percent of natural disaster events in 2011. Hydrological and geophysical events accounted for 19 and 3 disasters, respectively (see Figure 5).

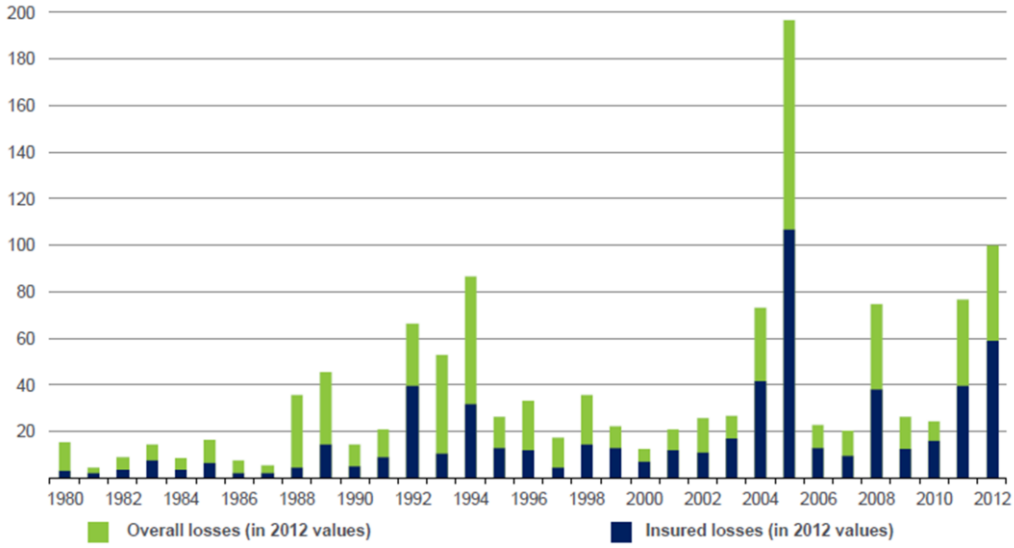
Figure 5. Frequency of Natural Disasters in the United States From 1980 to 2012



Source: Munich Re NatCatSERVICE, 2013.

Figure 6. Losses Due to Natural Disasters in the United States From 1980 to 2012

(in billion U.S. dollar)



Source: Munich Re NatCatSERVICE, 2013.

Even though the total number of natural disasters declined to 184 in 2012 compared to 250 events in 2010, 2012 experienced a much greater overall financial loss. The costs of natural disasters have been increasing considerably, largely due to increases in population, development, and wealth density, particularly in disaster-prone areas. For the United States, the year 2012 was

the costliest year since 2005 with approximately $100 billion in combined insured and uninsured losses due to natural disaster events (see Figure 6).[50] In 2012, the United States accounted for a high proportion of global natural disaster losses, accounting for some 67 percent of overall losses and 90 percent of insured losses.[51]

In Figure 6, blue bars indicate insured losses, and combined together, blue and green bars indicate overall economic losses. While losses varied significantly from year to year—largely due to the effects of catastrophic weather events such as hurricanes—the 30-year data on U.S. natural catastrophes from Munich Re's NatCatSERVICE, shows that the total economic losses have risen significantly from 1980 through 2012 (effects of inflation have been controlled in the figure). Particularly, the portion of insured loss has been growing gradually along with the development of businesses and infrastructure over the past few decades in the United States. In addition, there is a growing concern that a large portion of the U.S. population, business, and critical infrastructure may currently be underinsured, especially considering the recent observation of growing climate variability and impacts of natural disasters.

The most recent, significant meteorological event, Hurricane Sandy, which hit the East Coast in late October 2012, was no exception to creating a devastating loss. While economic impact assessments were still underway at the time of this report, Sandy was recorded as the third costliest hurricane in the U.S. history after Hurricanes Katrina (2005) and Andrew (1992).[52] Sandy was responsible for the deaths of 121 people in the United States (199 overall) and up to $25 billion in insured losses,[53] as the storm struck the most densely populated part of the country, including large areas of New York, New Jersey, and Pennsylvania.[54] However, the total economic loss from Hurricane Sandy is estimated to be three to four times the insured loss, and this difference between the insured and total economic losses may potentially be paid by the State and Federal governments.

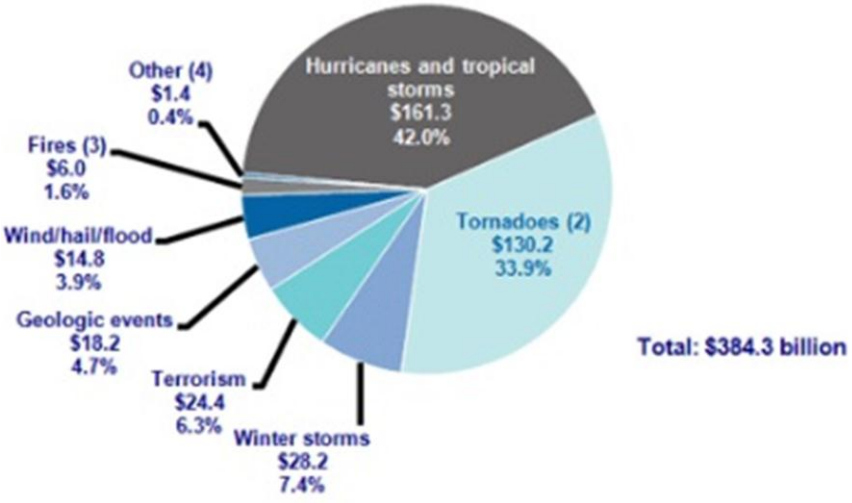
As of February 2013, Federal government authorized a total of $60.2 billion in Sandy disaster aid through two separate laws: On January 4, 2013, Congress passed a bill that gives the National Flood Insurance Program (NFIP) the authority to borrow $9.7 billion to meet claims stemming from damage caused by Hurricane Sandy and other disasters;[55] on January 28, 2013, Congress

[50] Munich Re NatCatSERVICE, 2012.
[51] "Munich Re: 2012 Natural Disasters Cost Global Insurers $65B Vs $119B," Wall Street Journal, January 3, 2013, http://online.wsj.com/article/BT-CO-20130103-701942.html (accessed February 5, 2013).
[52] Netter, F., President, Reinsurance Association of America, Presented December 14, 2012, http://files.eesi.org/121412_Frank_Nutter.pdf (accessed December 18, 2012).
[53] This estimate includes insured property and business interruption losses only, and the average of the midpoints of three risk modeler estimates is $18.8 billion. See http://files.eesi.org/121412_Frank_Nutter.pdf (accessed December 18, 2012).
[54] Holm, E., "Sandy May Cost Insurers Up to $25 Billion," Wall Street Journal, November 14, 2012, http://online.wsj.com/article/SB10001424127887324735104578119301366617508.html (accessed November 19, 2012).
[55] Hernandez, R., "Congress Passes a $9.7 Billion Storm Relief Measure," New York Times, January 4, 2013, http://www.nytimes.com/2013/01/05/nyregion/house-passes-9-7-billion-in-relief-for-hurricane-sandy-victims.html (accessed February 5, 2013).

passed another bill giving additional $50.5 billion towards recovery efforts.[56] In addition to the economic losses as a result of the physical damage inflicted by the storm, there are numerous cascading impacts in the U.S. economy, including lost retail sales, decreased industrial production, and lost income, due to the closure of many businesses in the affected region.[57] These factors contribute to the difficulty of assessing the overall loss of a disaster event.

According to the Insurance Information Institute, natural disasters were the primary cause for the majority of insured losses in the United States between 1991 and 2011, during which the Nation suffered approximately $384 billion in insured losses (see Figure 7).[58] Within the natural disaster category, tropical cyclones or hurricanes have long been the leading cause of losses and accounted for 42 percent of total catastrophe losses, followed by tornado and winter storm losses, which accounted for approximately 34 percent and seven percent, respectively.[59] Non-natural

Figure 7. Insured Catastrophe Losses by Cause of Loss in the United States From 1991 to 2011
(in billion 2011 U.S. dollar, inflation adjusted)



(1) Estimated property losses adjusted for inflation through 2011 by ISO using the GDP implicit price deflator. Excludes catastrophes causing direct losses less than $25 million in 1997 dollars. Does not include flood damage covered by the federally administered National Flood Insurance Program.

(2) Excludes snow.

(3) Includes wildland fires.

(4) Includes losses from civil disorders, water damage, utility service disruptions, and any workers compensation catastrophes generating losses in excess of PCS's threshold after adjusting for inflation.

Source: Insurance Information Institute and the Property Claim Services (PCS), 2012.

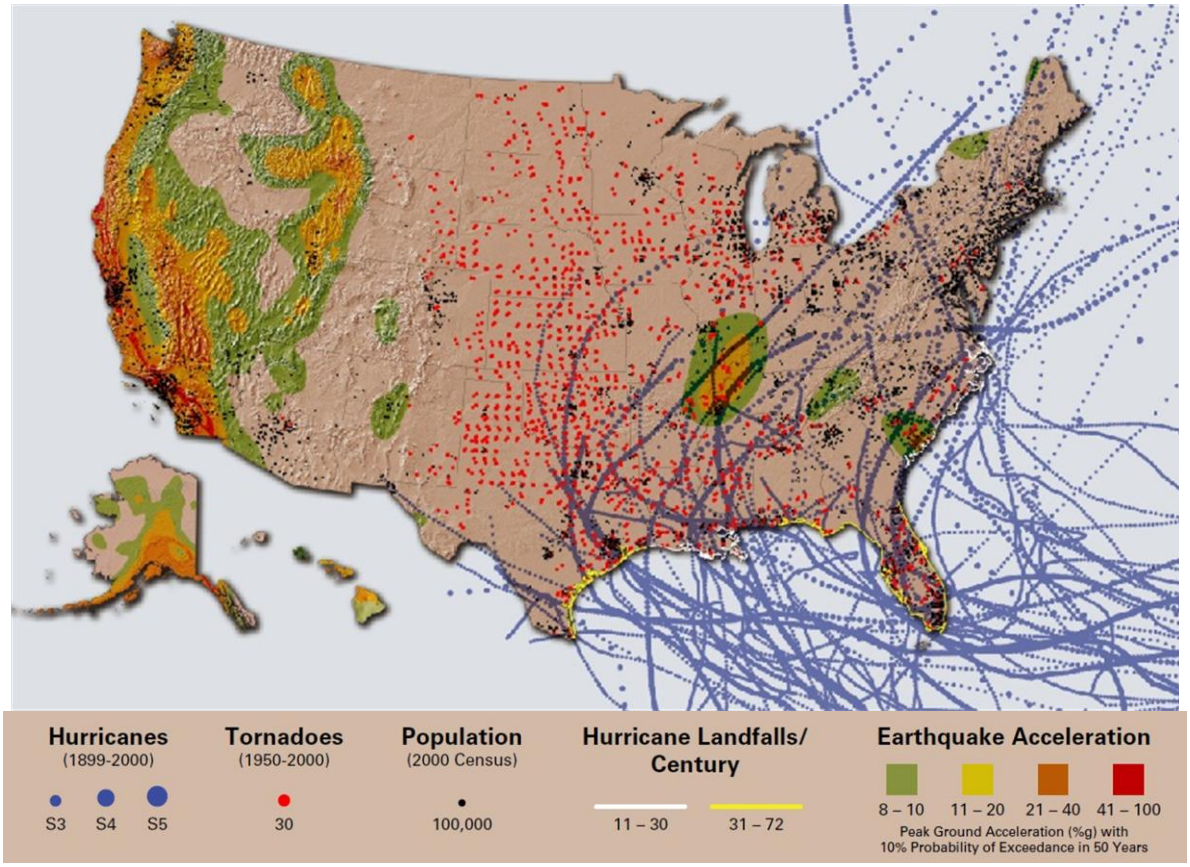
[56] Lawder, D., "Senate votes to approve $50.5 billion Sandy aid package," Reuters, January 28, 2013, http://www.reuters.com/article/2013/01/28/us-usa-congress-sandy-idUSBRE90R10620130128 (accessed February 5, 2013).
[57] Cox, J., "Sandy's Impact on Job Growth Will Be 'Acute': LaVorgna," November 19, 2012, CNBC http://www.cnbc.com/id/49883615 (accessed November 19, 2012). The storm cut power to more than 8 million homes, shut down 70 percent of East Coast oil refineries. Affected area produces about 10 percent of U.S. economic output. See http://business.time.com/2012/10/31/hurricane-sandy-estimated-to-cost-60-billion/ (accessed November 16, 2012).
[58] Insurance Information Institute, Inflation Adjusted U.S. Catastrophe Losses by Causes of Losses from 1991 to 2011, http://www.iii.org/index.cfm?instanceID=242789 (accessed August 23, 2012).
[59] Ibid.

catastrophes, including terrorism, fires, and others accounted for less than 10 percent of the total loss. See Appendix D for detailed assessment of natural disasters in the United States by type of events, including thunderstorm, winter storm, tropical cyclone, and burned acres in wildfire.

3.3 U.S. Vulnerabilities to Natural Hazards

Natural disasters are a result of the occurrence of natural events in the built environment, yet various reports suggest that population and infrastructure development are growing in potentially more environmentally vulnerable areas in the United States.[60] Figure 8 is a representation of natural hazard vulnerabilities in the United States. As shown here, the United States is exposed to several natural hazards, including earthquakes, hurricanes, and tornados. Specifically, the Pacific coastal areas face a considerable risk of earthquakes, and the Gulf of Mexico and South Atlantic face high risk of hurricanes. Tornados are the main natural hazard in the Great Plains. From a long term historical perspective, other areas experience considerable risks from

Figure 8. U.S. Vulnerability to Natural Hazards



Note: This map is a simplified illustration of various natural hazards occurring in the U.S. territory. Hurricanes—indicates paths of category 3, 4, 5 hurricanes between 1899 and 2000; Tornadoes—indicates the location most commonly hit by tornadoes; Population—indicates areas most heavily populated; Hurricane Landfalls/Century—yellow indicates regions experiencing 31 to 72 hurricane landfalls per century; white indicates regions experiencing 11 to 30 hurricane landfalls per century; Earthquake Acceleration—indicates Peak Ground Acceleration (%g) with 10% Probability of Exceedance in 50 Years.

Source: American Geosciences Institute, http://www.agiweb.org/gap/workgroup/USHazPoster.pdf.

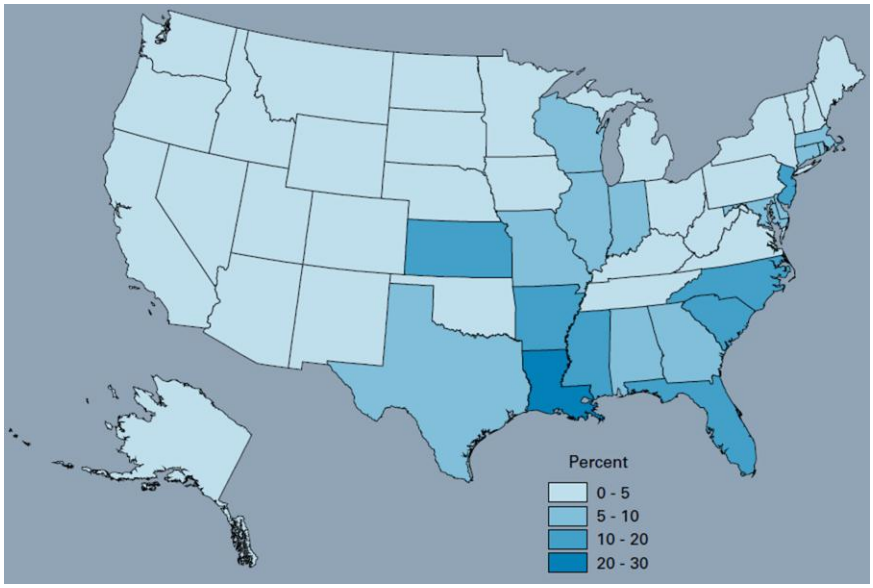
[60] "U.S. Vulnerability to Natural Hazards," American Geoscience Institute, http://www.agiweb.org/gap/workgroup/USHazPoster.pdf, (accessed September 2, 2012).

earthquake, flooding, drought, and possible space weather impacts.

Although coastal counties[61] constituted 17 percent of the total land area of the United States (not including Alaska), they accounted for 57 percent of the total U.S. population in 2008.[62] The total population of these counties has grown from 95 million in 1960 to 157 million in 2008, an increase of 67 percent.[63] Such an increase in population led to additional economic activities and infrastructure development to support the people and businesses which, as a result, could expose the population, properties, and infrastructure to damage from natural catastrophes.[64]

Figure 9 is a representation of floodplain by State. In addition to the States located in the Gulf of Mexico and the Atlantic Coast, a number of Midwestern States have a considerable amount of floodplain. A recent study stated, "floods are to the Midwest what hurricanes are to coastal areas—the region's most widely destructive type of regularly occurring natural disaster."[65]

Figure 9. Percent of Area in Floodplain by State



Source: American Geosciences Institute, http://www.agiweb.org/gap/workgroup/USHazPoster.pdf.

[61] The National Oceanic and Atmospheric Administration (NOAA) defines a county as coastal if "1) at least 15 percent of [the] country's total land area is located within the Nation's coastal watershed; or 2) a portion of [the] entire county accounts for at least 15 percent of a coastal cataloging unit." This definition is well suited for evaluating how human activities occurring inland can affect water- and habitat-quality along the coast. However, most of the counties are not adjacent to a body of saltwater, and these nonadjacent counties are sometimes not perceived as coastal. This definition is not to be confused with the term "coastline counties" used by the U.S. Census Bureau. To qualify as the U.S. Census Bureau's definition of a coastline county, a county has to be adjacent to water classified as either coastal water or territorial sea.

[62] "Population Trends Along the Coastal United States: 1980-2008," NOAA, September 2004, http://oceanservice.noaa.gov/programs/mb/pdfs/coastal_pop_trends_complete.pdf (accessed June 28, 2012).

[63] "Coastline Population Trends in the United States: 1960 to 2008," U.S. Census Bureau, May 2010, http://www.census.gov/prod/2010pubs/p25-1139.pdf (accessed June 28, 2012).

[64] "Managing the escalating risks of natural catastrophes in the United States," Lloyd's, 2011, http://www.lloyds.com/~/media/Lloyds/Reports/Emerging%20Risk%20Reports/Natural%20Catastrophes%20in%20the%20US.pdf (accessed July 19, 2012).

[65] "Doubled Trouble: More Midwestern Extreme Storms," The Rocky Mountain Climate Organization, May 2012, http://www.rockymountainclimate.org/images/DoubledTroubleHigh.pdf (accessed June 28, 2012).

Unlike the hurricanes being the main cause of flooding in the coastal States, the increasing frequency of large storms that bring heavy rain of three inches or more are blamed for the flooding in the Midwest.[66] Understanding such risks and vulnerabilities is essential to risk management, and insurance can be instrumental in identifying and communicating them.

3.4 Insurance's Role in Risk Mitigation and Extreme Events

Understanding and identifying risks is one of the main tasks and constitutes the heart of the insurance business.[67] The insurance industry must be able to estimate an event's occurrence and its associated economic damages with a certain level of reliability to effectively manage their insurance products and financial risks. With abundance of historical data on natural disasters and their economic impacts, the insurance industry has developed and maintained the technical and actuarial expertise for providing risk assessment and risk allocation mechanisms. Effective risk management generally involves a wide range of efforts to reduce and transfer risks as well as to respond to events and disasters, and the insurance industry applies risk management through identifying, assessing, modeling, and controlling risks in writing actual policies.[68] Such insurance instruments can be used to help households, business, and governments absorb the losses from disasters.

As discussed in Section 1.2, insurance provides a method to distribute and reduce the financial risk associated with certain adverse events, by sharing costs either between individuals or over time. The insurance industry can also have an important role in helping society to adapt and become more resilient to catastrophes and extreme events though the following ways:

- Helping customers and society better understand potential impacts by modeling climate or weather-related events and other potential, evolving threats and catastrophes;
- Providing economic incentives to encourage certain behaviors that can reduce risks and discourage those that can increase risks (e.g., a firm or an individual investing in security and mitigation measures should be eligible to receive lower insurance rates);
- Contributing to the collection of data on the costs relating to extreme events, as well as risk analysis and management;
- Promoting risk awareness, resilient reconstruction methods after losses, and adaptation solutions; and
- Providing market-based product options that include incentives to prevention, risk retention, and risk transfer mechanisms.[69]

3.5 Government and Public Insurance

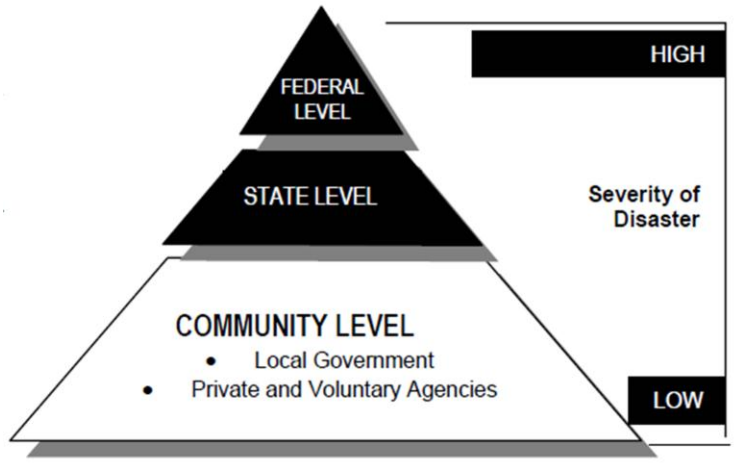
Natural disasters not only devastate communities and individuals but also can be costly to insurers and government organizations. The U.S. government often bears the key responsibilities for risk mitigation in society, and government organizations at all levels—Federal, State, local, tribal, and territorial—share the common goal of preventing or lessening the effects of disasters.

---

[66] Ibid.
[67] "Extreme events and insurance: 2011 annus horribilis," The Geneva Reports, Risk and Insurance Research, March 2012, http://www.genevaassociation.org/PDF/Geneva_Reports/GA-2012-Geneva_report%5B5%5D.pdf (accessed July 5, 2012).
[68] Ibid.
[69] "Global insurance industry fact-sheet," Geneva Association, 2011, http://www.genevaassociation.org/pdf/News/2011globalinsuranceindustryfactsheet.pdf (accessed July 5, 2012).

In disaster recovery and relief efforts, three levels of involvement—community, State, and Federal—are possible; however, only major disasters require extensive resources that result in requests for Federal assistance (see Figure 10). Thus, the Federal government is usually considered the "insurer of last resort" and bares the costs of natural disasters through disaster declarations and spending by FEMA.[70]

Figure 10. Hierarchy of Disaster Assistance



Source: FEMA, http://training.fema.gov/emiweb/downloads/IS7unit_1.pdf.

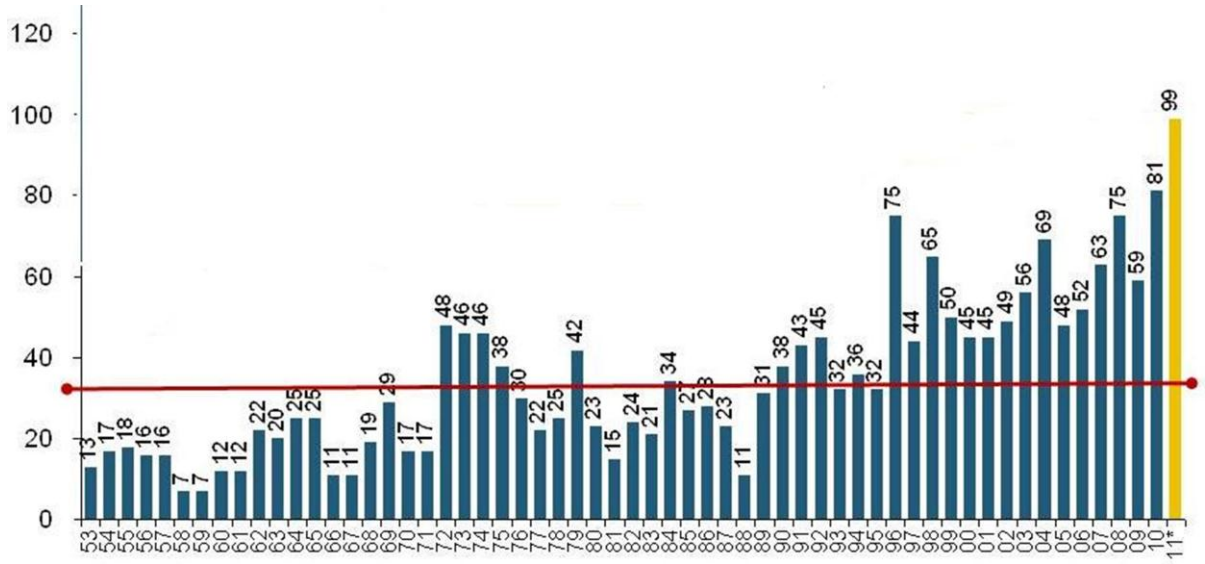
Between 1953 and 2010, the Federal government has made a total of 2,049 disaster declaration, averaging 34 declarations annually.[71] The number of presidential disaster declarations has generally increased over the last half century, however. Between 2004 and 2010, the Federal government made 539 declarations, or an average of 67 declarations a year. During these eight years, FEMA committed more than $80 billion for disaster recovery, half of which went to facilitate recovery from Katrina.[72] In 2011 alone, the Federal government declared 99 disaster disasters, breaking the previous record of 81 set in 2010 (see Figure 11). Two-thirds of the declaration in 2011 came from hurricanes and floods. The costs of natural disasters are driven by relatively few large events, however. One source estimated that less than one percent of disaster declarations are responsible for the majority of the costs.[73] (See Appendix E for the Federal emergency declaration process.)

The Federal government, through 30 different organizations, operates at least 157 programs that provide insurance-like benefits to individuals and businesses (see Appendix G for a full listing of the Federal insurance activities).[74] The Federal government engages in a wide variety of insurance activities and has assumed insurance risks for at least two reasons: (1) the government may step in when insurance is not widely available because private insurers cannot collectively absorb or affordably price the insurance risk; or (2) the Federal government has self-insured—

[70] "The Increasing Costs of U.S. Natural Disasters," Geotimes, The Princeton University, November 2005, http://www.geotimes.org/nov05/feature_disastercosts.html (accessed July 23, 2012).
[71] FEMA, Declared Disasters by Year or State, http://www.fema.gov/news/disaster_totals_annual.fema (accessed June 28, 2012).
[72] GAO, Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own, GAO-12-838, September 2012, http://www.gao.gov/assets/650/648162.pdf (accessed November 19, 2012).
[73] "The Increasing Costs of U.S. Natural Disasters," Geotimes, The Princeton University, November 2005.
[74] GAO, Natural Disasters: Public Policy Options for Changing the Federal Role in Natural Catastrophe Insurance, GAO-08-7, November 2007.

that is, elected to pay for losses itself when it has determined that doing so is preferable to purchasing insurance in the private market.[75]

Figure 11. Number of Federal Disaster Declarations From 1953 to 2011



Source: Insurance Information Institute, Federal Emergency Management Administration, http://www.iii.org/assets/docs/ppt/Federal%20Disaster%20Declarations.ppt.

Among the many Federal insurance programs, two of the largest programs are the National Flood Insurance Program (NFIP), which insures properties at risk of damage from flooding, and the Federal Crop Insurance Corporation (FCIC), which insures crops that are vulnerable to drought, floods, or other natural disasters. (See Appendix F for the historical data pertaining to the NFIP and the FCIC.)

Congress authorized the NFIP in 1968 to minimize the economic impact of flooding events by providing flood insurance to individuals and businesses, because the U.S. private insurance industry believed flood risk was uninsurable.[76] Insurers were concerned with their ability to correctly price the product due to the problems of adverse selection (i.e. only highly exposed individuals will want coverage that would lead to high concentration of risk) and possible catastrophic losses.[77] The NFIP has been reauthorized many times since the program's inception, and the latest reauthorization was signed by President Barack Obama in July 2012.

The Federal crop insurance program began in 1938 when Congress authorized the FCIC as an experiment to address the effects of the Great Depression and crop losses seen in the Dust

[75] GAO, Catalogue of Federal Insurance Activities, GAO-05-265R, March 4, 2005, http://www.gao.gov/assets/100/93046.pdf (accessed September 24, 2012).
[76] While considered uninsurable in the United States, the insurers in other nations do offer private flood insurance coverage.
[77] King, Rawle P, "National Flood Insurance Program: Background, Challenges, and Financial Status," Congressional Research Services, July 1, 2011, http://www.fas.org/sgp/crs/misc/R40650.pdf (accessed August 9, 2012).

Bowl.[78] The Federal crop insurance program was permanently authorized by the Federal Crop Insurance Act of 1980 (P.L. 96-365).[79] By insuring crops that are vulnerable to natural disasters, the FCIC provides producers with risk management tools to address crop yield and/or revenue losses on their farms.

In addition to the disaster relief effort, the government plays a vital role in ensuring the viability of private insurance by creating appropriate legislative and regulatory frameworks.[80] While the Federal government retains the authority to regulate insurance, the primary responsibility for insurance regulation lies with the States, in accordance with the McCarran-Ferguson Act of 1945.[81] Per this act, State insurance commissioners are responsible for most aspects of insurance regulation.

In addition to being a regulator, States also offer a wide variety of public insurance programs. Although State-regulated disaster insurance programs have continued to grow, they are also facing a number of challenges. Critics of State-regulated disaster insurance programs have argued that insurance prices and terms of coverage are highly regulated and that the insurance industry is generally not allowed to respond freely to changing risks or market conditions. The result, it is argued, is that some States are creating a significant financial exposure that sometimes may not be covered by the revenues that they earn through low-priced insurance policies. According to a recent analysis by the Insurance Information Institute in 2011, more than 35 programs nationwide had grown to provide a record-high of 3.3 million policies, many of which are in high-risk regions.[82] Despite attempts by certain States to reduce the size of their plans, "this market of last resort remains the market of first choice for many vulnerable, high-risk coastal properties."[83] Similar concerns were raised about the NFIP, which has faced criticism that flood planning is based on historical data instead of future projections that take into account the effects of climate change—rising sea levels, increased flooding due to intense precipitation events, and an increase in the intensity and occurrence of hurricanes.

Such concerns about the NFIP may be improving in the near future, however. The Biggert—Waters Flood Insurance Reform Act of 2012, which reauthorized the NFIP until September 2017, included provisions that could help State and local governments implement policies to adapt to sea-level rise and other flood impacts from climate change. Some of the key provisions included:

- A requirement that premiums be calculated based upon "average historical loss year," including catastrophic loss years;

[78] "Dust Bowl" refers to a period of severe dust storms caused by severe drought conditions in the United States in the 1930s. Shields, D. A. "Federal Crop Insurance: Background and Issues," Congressional Research Service, December 13, 2010, http://www.nationalaglawcenter.org/assets/crs/R40532.pdf (accessed August 10, 2012).
[79] Ibid.
[80] "Critical Information Infrastructure: The digital economy's Achilles heel," CRO Forum, November 2008, http://www.thecroforum.org/assets/files/publications/CRO%20Position%20Paper%20-%20Critical%20Information%20Infrastructure.pdf (accessed July 18, 2012).
[81] Pub. L. No. 79-5, Ch. 20, 59 Stat. 33 (1945) codified as amended at 15 U.S.C. §§ 1011-1015. See also GAO, Ultimate Effects of McCarran-Ferguson Federal Antitrust Exemption on Insurer Activity Are Unclear, GAO-05-816R (Washington, D.C.: July 28, 2005).
[82] "State insurance programs continue to grow amid hurricane lull," E&E News, July 12, 2012, http://eenews.net/public/climatewire/2012/07/12/1 (accessed August 15, 2012).
[83] Ibid.

- The establishment of an advisory to consider the impacts of sea-level rise in flood insurance rate maps (FIRMs);
- The update of FIRMs to include "relevant information and data" on flood hazards caused by land-use changes, and "future changes in sea levels, precipitation, and intensity of hurricanes"; and
- A study on using reinsurance to manage financial risks associated with flooding and options for privatizing the NFIP.[84]

IV. Selected Risks in the Energy Sector

The Energy Sector consists of widely-diverse and geographically-dispersed critical assets and systems that are interdependent of one another. Many aspects of the Energy Sector, including the operation of energy infrastructure as well as the supply and delivery of electricity and fuels, are sensitive to weather events and climate variability. Energy infrastructure consists of large and costly fixed assets with long lifetimes, which are potentially vulnerable to impacts associated with climate events. The ability of this infrastructure to function properly despite climate variability and extreme weather events is critical, especially during recovery from a natural disaster, because many critical infrastructure and functions—hospitals, water systems, transportation, and telecommunication—depend on the reliable supply and delivery of electricity and other fuels for operation. For these reasons, this section explores the various natural hazards that the Energy Sector faces, and what impacts they might have on the operation and reliability of critical energy infrastructure.

4.1 Electricity Sector

Energy infrastructure, particularly the electric power grid, is one of the Nation's critical life-line infrastructure on which many other critical infrastructure depend, and the destruction of this infrastructure can cause a significant impact to national security and the U.S. economy. The operation of electric power infrastructure, including the production and delivery of electricity is susceptible to climate variability. For example, the rise and fall of temperature influences electric power consumption, while the episodic and long-lasting regional availability of water supply can constrain different forms of energy production. Specifically, water scarcity, changing precipitation patterns, warmer average temperatures, and greater variability in water supply affect the generation of hydropower, as well as the operation of nuclear and fossil fuel power plants, which require high quality and quantities of water for cooling.[85] Warmer average air temperatures and more frequent and severe heat waves can lead to a greater use of air conditioning and increased power demand (particularly during the peak demand) in the summer; increased air temperatures can also lead to greater losses in transmission and distribution

[84] Grannis, J. "Analysis of How the Flood Insurance Reform Act of 2012 (H.R. 4348) May Affect State and Local Adaptation Efforts," Georgetown Climate Center, August 14, 2012, http://www.georgetownclimate.org/sites/default/files/Analysis%20of%20the%20Flood%20Insurance%20Reform%20Act%20of%202012.pdf (accessed August 16, 2012).

[85] "Dams and Energy Sectors Interdependency Study," U.S. Department of Energy, U.S Department of Homeland Security, September 2011, http://energy.gov/sites/prod/files/Dams-Energy%20Interdependency%20Study.pdf (accessed November 7, 2012).

systems.[86] In addition, new, intermittent energy technologies such as wind and solar are also expected to present new challenges, and in some cases, the use of these technologies can increase the risk of power brownout. Therefore, the adaptation of critical infrastructure to unexpected weather variability is critical to maintaining infrastructure stability, adequate fuel supply, as well as the grid and electricity delivery reliability.

Extreme weather events, including flooding, storm surge, wild fire, heavy rains, and hurricanes can cause physical damage to power generation, transmission, and distribution facilities and related infrastructure. Different types of natural disasters impact these segments differently; however. The variety of impacts can be attributed to the fact that generation and transmission systems consist of large, clustered assets in generation facilities and in substations, whereas distribution assets are spread over wide, geographical areas. For example, the snow storm that hit the Northeast in 2010 was largely a distribution problem in which tree limbs fell onto the local power lines, and little or no impact was seen at generation facilities.

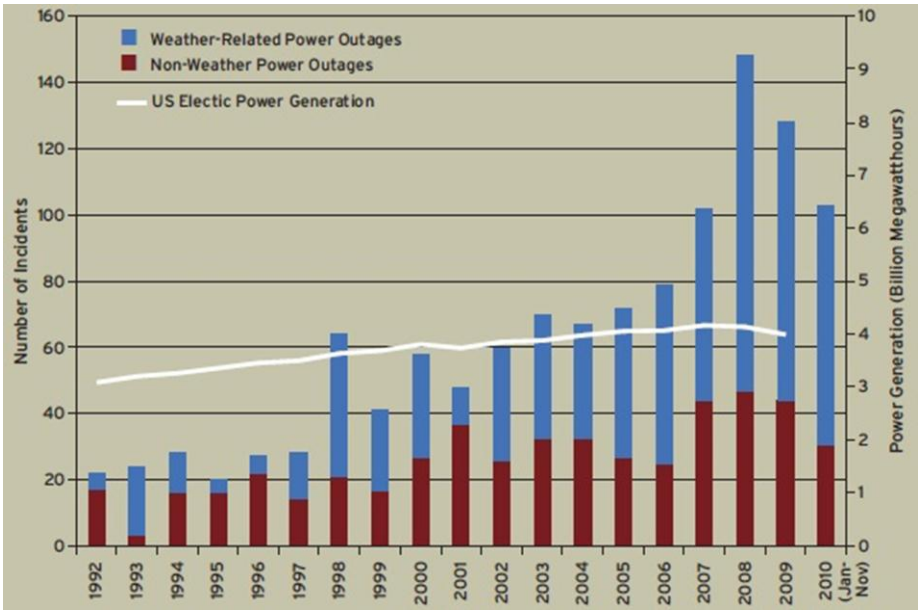
Even though the total electric power generation in the United States increased modestly between 1992 and 2010, large-scale[87] power outages increased significantly during the same period, according to data from the U.S. Energy Information Administration and the North American Electric Reliability Corporation (NERC) (see Figure 12). Weather-related events affected the highest number of customers, or 180,000 customers on average, as compared to about 50,000 customers for non-weather incidents (excluding the August 2003 Northeast blackout).[88]

With mounting costs of power disruptions, electric utilities are incurring substantial costs to repair their assets and systems after disasters strike. The financial impact of disaster restoration can be devastating if it is not mitigated effectively, as some companies can experience restoration costs exceeding net operating income for the year. Several methods are currently used by utilities to lessen the financial impact of disaster restoration costs. Yet there is little consistency in how these methods are applied throughout the industry, or even within a company, from disaster to disaster.[89] In some jurisdictions, State public service or utility commissions will order ratepayer-funded cost recovery for substantial portions of utilities' claimed restoration costs although the time required for many utilities to recover costs through regulatory processes can result in short term borrowing. In addition, due to the lack of commercially-available insurance at affordable rates, some utilities elect to self-insure to pay for major storms or purchase short-term catastrophe coverage. However, some utilities may not have

[86] "Physical Risks from Climate Change: A guide for companies and investors on disclosure and management of climate impacts," Ceres, May 2012, http://www.ceres.org/resources/reports/physical-risks-from-climate-change (accessed June 27, 2012).
[87] According to the definition by the North American Electric Reliability Corporation (NERC), "large-scale disruption" is defined as a power outage that affects at least 50,000 customers for at least 1 hour or a loss of at least 300 MVA for at least 15 minutes.
[88] "More Extreme Weather and the U.S. Energy Infrastructure," National Wildlife Federation, 2011, http://www.nwf.org/~/media/PDFs/Global-Warming/Extreme-Weather/Final_NWF_EnergyInfrastructureReport_4-8-11.ashx (accessed June 29, 2012).
[89] "After the Disaster: Utility Restoration Cost Recovery," Edison Electric Institute, February 2005, http://www.eei.org/ourissues/electricitydistribution/Documents/Utility_Restoration_Cost_Recovery.pdf (accessed August 21, 2012).

sufficient reserves or credits to pay for catastrophic storms or provide a ready source of cash to pay for storms-related costs.[90]

Figure 12. Major Electric Power Disruptions in the United States Between 1992 and 2010



Note: Disruptions in the chart were tabulated by hand from annual reports issued by the North American Electric Reliability Corporation and include outages and public appeals to reduce electricity consumption. Note that utilities are only required to report large-scale disruptions (e.g., those affecting at least 50,000 customers for at least 1 hour or a loss of at least 300 MW for at least 15 minutes). This chart does not include outages in local distribution networks, which are much more common but affect fewer people. Note that the 2010 data is preliminary and does not include public appeals.

Source: National Wildlife Federation, 2011, based on data from North American Electric Reliability Corporation and the U.S. Energy Information Administration.

4.1.1 Power Blackout Risks

Infrastructure owners are not directly exposed to the full costs that the society bears due to infrastructure failure. In other words, an electric utility does not bear the full societal costs incurred by the customers due to power interruption. Thus the losses incurred by individuals and companies due to power outage can be much larger than the cost of repairing the damage.

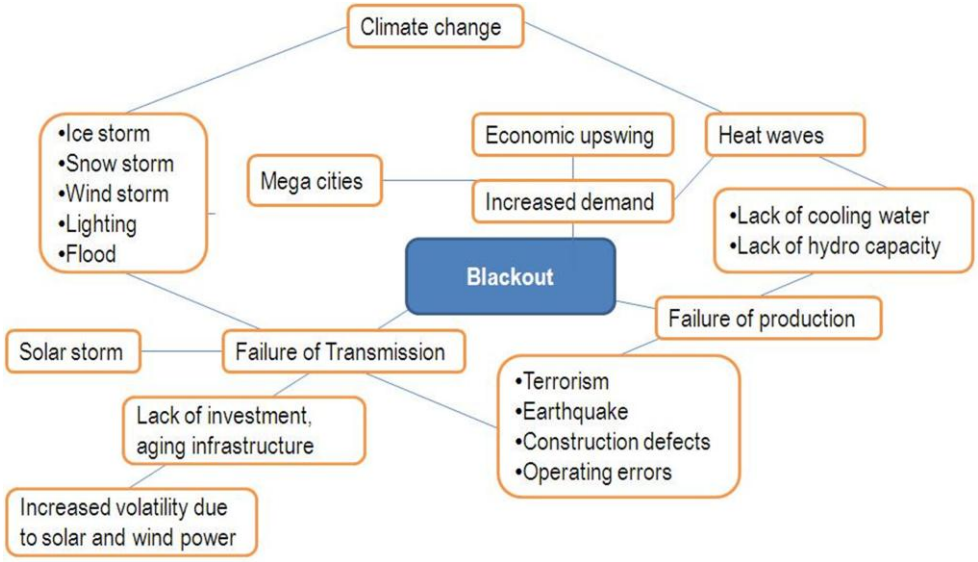
Power outages in the United States during the last decade have demonstrated an increasing likelihood of regional and long-lasting blackouts resulting in high economic losses. Due to the growing interconnectedness in combination with aging infrastructure, this risk is expected to increase in both frequency and severity. As such, the CRO Forum—a group of professional risk managers who focus on developing and promoting industry best practices in risk management—has identified power blackout as one of emerging risks.[91]

[90] Ibid.

[91] The CRO Forum launched the Emerging Risks Initiative in 2005 to raise awareness of major emerging risks relevant to society and the (re)insurance industry. In 2012 the initiative will be chaired by Hannover Re and consists of eight members representing Allianz, AXA, Generali, Hannover Re, Munich Re, RSA, Swiss Re and Zurich Financial Services Group. See http://www.thecroforum.org/emerging_risks_initiative.html (accessed September 13, 2012).

There are numerous potential causes for power blackouts, including storms, transmission failure, heat waves, and aging infrastructure to name a few (see Figure 13). Relatively short term power disruptions (a few hours to a few days) are experienced frequently on a local or regional level around the world (e.g., caused by natural catastrophe events like earthquakes, storms, floods or heat waves). However, societies may not be familiar with large scale, long-lasting, power blackouts, caused by high-impact, low-frequency events[92] such as space weather or coordinated cyber or physical attacks. See Section 5 of this report for further discussion on these risks.

Figure 13. Potential Causes of Power Blackouts

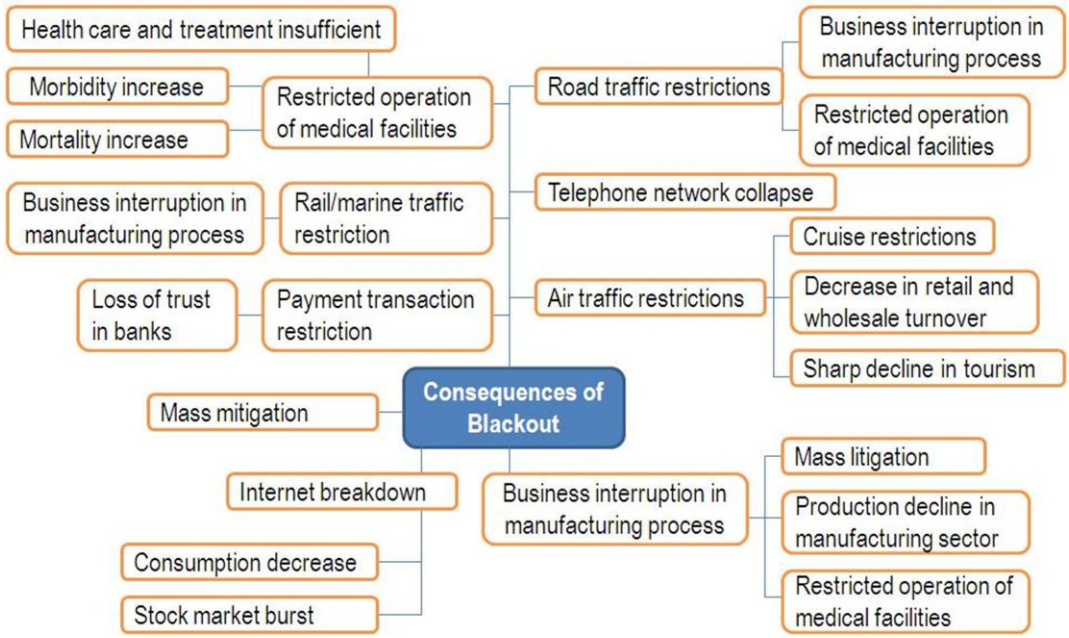


Source: Allianz, 2011.

These high-impact and low-frequency events can cause wide-ranging blackouts that can have a significant impact that are far reaching and affecting other critical infrastructure that is vital to human life and the economy. Figure 14 is an illustration of selected potential consequences of a blackout. Current risk management mechanisms, however, may not be adequate to mitigate losses following such a blackout. That is because risk transfer via insurance has usually required physical damage to either the insured's assets or the assets of specific service providers to trigger a business interruption claim. However, only 20 to 25 percent of business interruptions are related to a physical loss,[93] which means that should a major power blackout occur, even insured persons or businesses could potentially face a significant uninsured loss. To better mitigate such potential losses, new risk transfer solutions related to power blackout risks from current and evolving threats may be needed. Section 5.3 provides further discussions on the insurance mitigation options.

[92] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," NERC, June 2010, http://www.nerc.com/files/HILF.pdf (accessed March 25, 2013).
[93] "Japan Disaster Highlights the Need for Supply Chain Insurance," BestWire Services, March 28, 2011, http://fpn.advisen.com/articles/article140935191888258975.html (accessed August 19, 2012).

Figure 14. Selected Consequences of Power Blackouts



Source: Allianz, 2011.

Analyses of historic blackout events in the United States show that in 2008, the average electric customer interruption costs for medium and large industrial clients was between roughly $15,000 for a 30-minute blackout and approximately $93,000 for an eight-hour interruption.[94] The costs of power outage widely vary depending on the sector, however. For example, during an eight-hour event, agricultural firms have the lowest average cost of some $41,000 per event, whereas construction firms have the highest average cost of approximately $214,000 per event.[95] This data suggests the value of tailored risk management solutions for different industries and geographical locations. Physical damage to premises or distribution lines of electricity producers and distributors are likely to remain the main exposures.[96] Additional elements of nonphysical damage coverage may be designed in the future to accommodate specific needs of industrial and commercial sectors. Perils that could suit such a purpose include a lack of cooling water for power plants due to extended periods of drought or interruption of electricity production due to safety measures required by public authorities that may delay or slow restoration and recovery.[97]

4.2 Oil and Natural Gas Sector

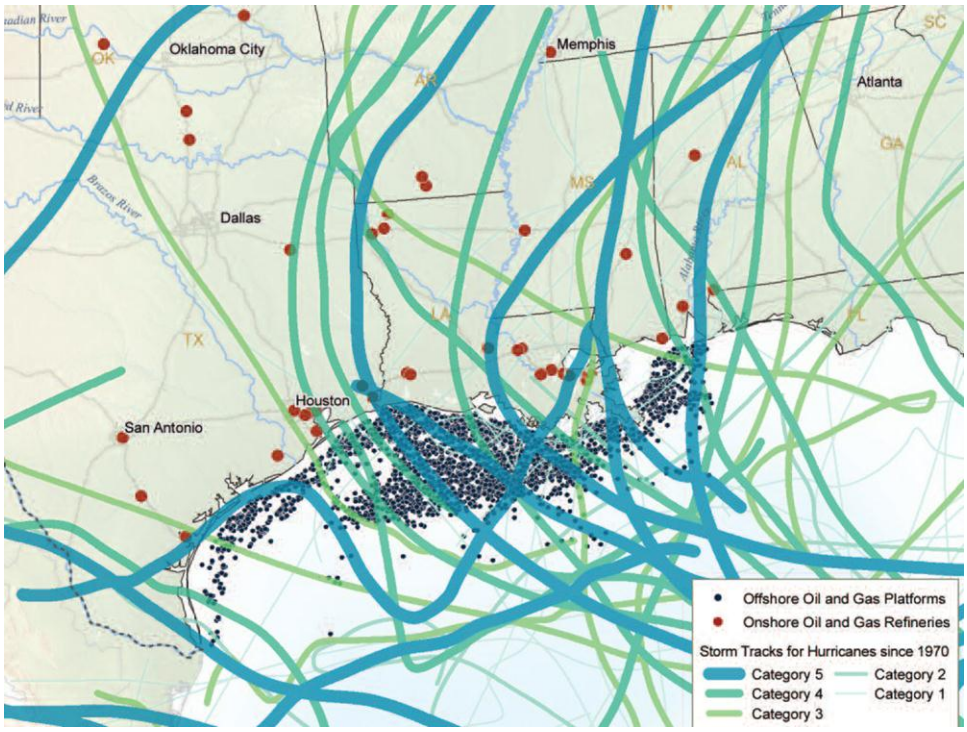
Even more so than electric power infrastructure, oil and natural gas infrastructure often operate in hazardous conditions such as deepwater and the ocean, as well as in locations that are prone to extreme weather events. The extensive oil and natural gas infrastructure located in the Gulf of

[94] All cost estimates in this paragraph are in 2008 U.S. dollar. "Estimated Value of Service Reliability for Electric Utility Customers in the United States," Lawrence Berkeley National Laboratory, June 2009, http://certs.lbl.gov/pdf/lbnl-2132e.pdf (accessed August 18, 2012).
[95] Ibid.
[96] "Blackout Risks," Allianz, November 2011, http://www.agcs.allianz.com/assets/PDFs/Special%20and%20stand-alone%20articles/Power_Blackout_Risks.pdf (accessed August 19, 2012).
[97] Ibid.

Mexico region is vulnerable to hurricanes and tropical storms. Since 1970, about two dozen major hurricanes in categories between three and five have made landfall on the shores of Texas, Louisiana, Mississippi, and Alabama—the four States where both off-shore and onshore oil and natural gas infrastructure is concentrated (see Figure 15). Hurricanes can have a devastating effect on oil and natural gas infrastructure, brought by flooding, lighting, wind, waves and mudslides. Appendix H summarizes some of the impacts of hurricanes damages to oil and natural gas infrastructure.

For the oil and natural gas sector, refining is more geographically dispersed than production. There are some 4,000 offshore oil and gas platforms, 31,000 miles of pipeline, and more than 25 onshore refineries in the coastal States bordering the Gulf of Mexico.[98] While production infrastructure is concentrated in the Gulf Coast, refining facilities are spread from Corpus Christi, Texas to Pascagoula, Mississippi. Thus it would be difficult for a single natural disaster to significantly impact the capability of and supply from the entire region. Nonetheless, this oil and natural gas infrastructure is not only at risk from natural hazards, but is also aging and may become more susceptible to the hurricane-related hazards of storm surge, flooding, and extreme winds. The greatest danger to most refineries has been the loss of power during a storm and the damage caused by that loss of power. Another challenge facing the industry is retrofitting this existing infrastructure with advanced technology to improve efficiency and resilience.[99]

Figure 15. Oil and Natural Gas Infrastructure Locations and Hurricane Paths



Source: National Wildlife Federation, 2011.

[98] "More Extreme Weather and the U.S. Energy Infrastructure," National Wildlife Federation, 2011, http://www.nwf.org/~/media/PDFs/Global-Warming/Extreme-Weather/Final_NWF_EnergyInfrastructureReport_4-8-11.ashx (accessed June 29, 2012).

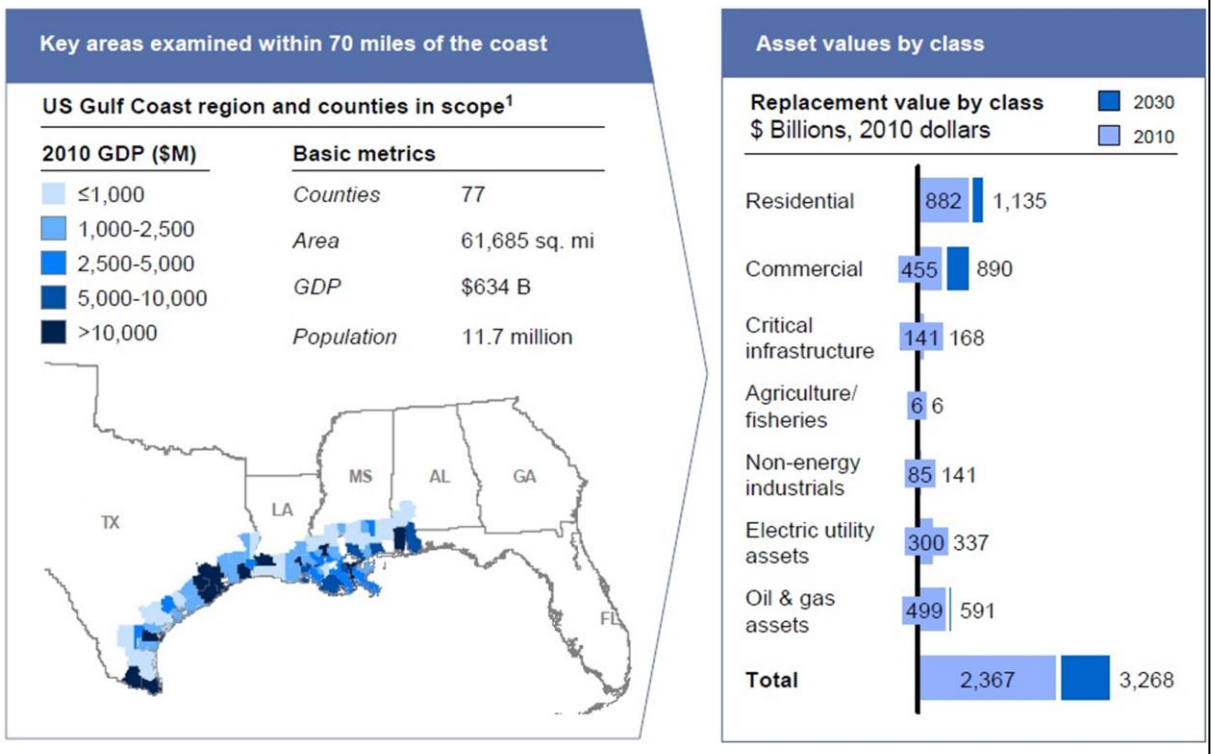
[99] "Hardening and Resilience: U.S. Energy Industry Response to Recent Hurricane Season," U.S. Department of Energy, August 2010, http://www.oe.netl.doe.gov/docs/HR-Report-final-081710.pdf (accessed August 23, 2012).

In addition to the possible increase in the severity and frequency of storms, oil and natural gas infrastructure in certain isolated areas can also be affected by regional drought conditions and water scarcity. Water availability can be a constraint for oil sands extraction and refining, for potential oil shale production, and for oil refineries that require large amounts of process steam and cooling water. In addition, water can be a significant problem in certain areas where rivers are used to transport products. Recent experience suggests that the United States may in the future experience more frequent events where rivers become too low to transport barges and fuels.

4.3 A Case Study: Building a Resilient Energy Gulf Coast

In 2010, DOE/OE conducted research to identify specific industry efforts related to storm hardening and resilience.[100] Specifically, the 2010 DOE/OE study focused on the measures that refiners, petroleum product pipeline operators, and electric utilities in the Gulf Coast have taken to harden their assets and make energy supply to the Southeast more resilient. The study identified numerous hardening and resilience activities that energy infrastructure owners and operators have undertaken in response to the 2005 and 2008 hurricane seasons. Hardening activities included flood and wind protection measures, as well as modernization of infrastructure systems and technologies. Resilience activities included general readiness measures such as preparing and updating hurricane preparation plans as well as storm-specific measures such as securing fuel supply or storage. (See Appendix I for the summary of energy hardening and resilience activities identified in this study.)

Figure 16. Scope of Analysis in the U.S. Gulf Coast Region



Source: Entergy Corporation, 2010.

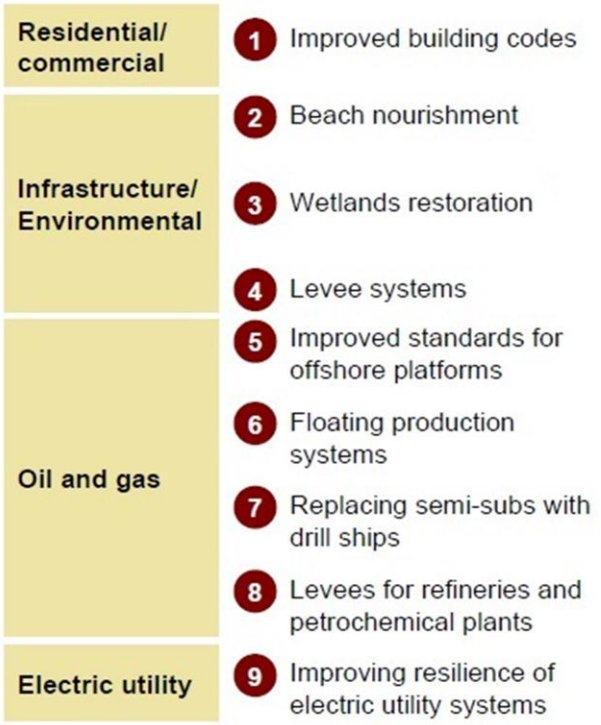
[100] Ibid.

In addition to implementing these various hardening and resilience measures, energy infrastructure owners and operators are increasingly integrating climate risk assessment performed by the insurance industry in their effort to build a more resilient business environment. A recent study by Entergy Corporation (Entergy) highlighted the approaches for developing a framework to address and quantify climate risks in the Gulf Coast. In a 2010 study entitled, "Building a Resilient Energy Gulf Coast," Entergy sought contribution from Swiss Re, which brought its natural catastrophe and climate risk assessment knowledge to quantify climate risks.[101] The scope of the analysis included 77 coastal counties in southern Texas, coastal Mississippi, and Alabama, where a considerable amount of critical infrastructure—including an estimated value of $300 billion in electricity assets and $499 billion in oil and natural gas assets—is located (see Figure 16). The area of study included approximately 11.7 million people and an annual GDP of $634 billion, with a total estimated replacement asset value of $2,367 billion in 2010.

The analysis of expected loss over time included the magnitude of the hazard, the economic value of assets at risk from the hazard, and the vulnerability of those assets to the hazard. The analysis showed that the Gulf Coast faced significant potential losses, with an estimated average annual loss of $14 billion in 2010, which was expected to increase to $18 billion per year by 2030 without considering any climate change. This number would be higher if climate change factors were incorporated.

To address such expected losses, the analysis presented potential measures to mitigate and prevent risks, including financial measures through insurance instruments. The study recommended specific measures to reduce risk across four sectors—residential and commercial, infrastructure and environmental, oil and natural gas, and electric utility (see Figure 17).

Figure 17. Recommended Measures to Reduce Risks



Source: Entergy Corporation, 2010.

Finally, the Entergy study suggested that for extreme events, insurance or risk transfer measures were more cost-efficient than physical measures in providing coverage. It also found that four risk transfer actions could help address residual loss through insurance: increasing penetration of existing insurance (through more affordable premiums that are linked to physical measures), decreasing the prevalence of underinsurance (through incentives that encourage updating of

[101] "Building a Resilient Gulf Coast: Executive Report," Entergy Corporation, 2010, http://www.entergy.com/content/our_community/environment/GulfCoastAdaptation/Building_a_Resilient_Gulf_Coast.pdf (accessed August 20, 2012).

insured value of property), encouraging additional self-insurance, and transferring top-layer risk (through catastrophe bonds).[102]

V. Emerging Risks in the Energy Sector

In addition to the natural disaster risks that have affected energy infrastructure for centuries, the Energy Sector faces new, emerging risks that threaten the operation and resilience of its critical infrastructure. As defined in Section 2 of this report, an "emerging risk" indicates that the frequency and consequence of the risk is uncertain or unknown. Because of the challenge the insurance industry faces in understanding and quantifying such a risk, it is difficult for the energy industry to use insurance instruments as an appropriate risk management tool for emerging risks.

For the insurance industry, emerging risks present a considerable challenge, as they are perceived to be potentially significant but may not be fully understood or addressed in existing insurance terms and conditions.[103] Although the potential loss can be large, emerging risks are characterized by a high degree of uncertainty and lack of basic information to adequately assess the frequency and severity of the risk. To minimize the impact, it is important to identify, analyze, quantify, and communicate the reality of emerging risks and to foster a stakeholder dialogue with representatives of a community that shares such risks.[104] However, due to the lack of available data, pricing and clarifying insurance coverage and products remains a challenge for the insurance industry.

In case of terrorism risk, following the September 11 attacks, the U.S. government created the Federal Terrorism Insurance Program (FTIP) in 2002 to help the insurance market recover from 9/11 and create transitional period for private insurance markets to stabilize and develop solutions to insuring terrorism.[105] The Terrorism Risk Insurance Act (TRIA) of 2002, which created the FTIP, was reauthorized in 2007 to extend the FTIP through December 31, 2014. While it may not be an entirely new threat, terrorism risk continues to be a concern for the Energy Sector.

In this section, selected emerging risks—cybersecurity and space weather events—in the Energy Sector are examined, including what the risks involve, how the insurance industry perceives such risks, and the challenges in effectively managing them through insurance mechanisms.[106]

5.1 Cybersecurity Risks

Cybersecurity risk has been a concern for the Energy Sector for quite some time, due to the sector's increasing dependence on advanced technology.[107] With the Energy Sector's increased

[102] Ibid.
[103] "Emerging Risks Management at Lloyd's," Lloyd's, December 15, 2011, http://www.theirm.org/events/documents/NSmithpresentation.pdf (accessed August 3, 2012).
[104] "Critical Information Infrastructure: The digital economy's Achilles heel," CRO Forum, November 2008, http://www.thecroforum.org/assets/files/publications/CRO%20Position%20Paper%20-%20Critical%20Information%20Infrastructure.pdf (accessed August 5, 2012).
[105] For more information about the Federal Terrorism Insurance Program, see "Terrorism Risk Insurance Program," U.S. Department of Treasury, http://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx (accessed February 7, 2013).
[106] "Future Risks Take Shape in 2011," Lloyd's, January 10, 2011, http://www.lloyds.com/News-and-Insight/News-and-Features/360-News/Business-360/Future-risks-take-shape-in-2011 (accessed August 23, 2012).

connectivity and the interdependency within it, as well as across other sectors, companies are increasingly vulnerable to a variety of cybersecurity risks, including system failures, data losses, and cyber attacks. A single vulnerability can trigger cascading failures of critical infrastructure and networks and can create serious operational, financial, intellectual property, legal, regulatory and reputational issues.[108] As such, the World Economic Forum,[109] an international independent entity consisting of leading re/insurance and risk management organizations, identified cybersecurity as one of the top five global risks in its annual Global Risks Report in 2011 and 2012,[110] as did the Commercial Risk Europe's 2011 Risk Frontier Survey.[111]

Cyberspace is defined by its ubiquitous connectivity, and it is this connectivity that exposes critical infrastructure to the vulnerability of supply chain disruptions—physical and nonphysical interruptions resulting from a technology or network failure—which are not necessarily addressed by traditional insurance.[112] Further, outsourcing of information technology (IT) functions offshore, the use and connectivity of personal devices in a company-wide network, and the increasing use of cloud computing are some of the trends that present new dimensions in the cybersecurity risks. One of the biggest threats in these cases is that data is taken outside the traditional physical parameters of the office and outside of the company's control, in which a cybersecurity breach could happen without the company's knowledge. Therefore, protecting cybersecurity of critical infrastructure—utilities, telecommunications, financial services, and other systems—and what the various insurance mechanisms can do to help protect it remains a significant challenge.

This section highlights the growing cybersecurity risks and their economic impacts as assessed by various sources, as well as the challenges in addressing the protection and insurance measures against cybersecurity risks.

> "A cyber attack could adversely affect the companies. The utilities and other operators of critical energy infrastructure may face a heightened risk of cyber attack. In the event of such an attack, the utilities and the competitive energy businesses could have their operations disrupted, property damaged and customer information stolen; experience substantial loss of revenues, response costs and other financial loss; and be subject to increased regulation, litigation and damage to their reputation."
>
> - Consolidated Edison of New York, Quarterly report (10-Q), November 2011

[107] See the Energy Sector Specific Plan, which mentioned cyber security more than 40 times, the 2011 Energy Sector Annual Report, which mentioned cybersecurity almost 100 times and has a designated section on this evolving threat (pp.33-36 and p.52).
[108] Ibid.
[109] World Economic Forum, http://www.weforum.org/ (accessed November 28, 2012).
[110] Global Risks 2011, Sixth Edition, World Economic Forum, http://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf; Global Risks Report, Seventh Edition, World Economic Forum, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf (accessed September 17, 2012). The annual reports were developed in collaboration with the following organizations: Marsh & McLennan Companies; Swiss Reinsurance Company; Wharton Center for Risk Management; University of Pennsylvania; and Zurich Financial Services.
[111] Commercial Risk Europe is the only pan-European newspaper dedicated to news, trends and issues critical to corporate risk and insurance management executives across Europe. It annual publication, Risk Frontier Survey, gauges the state of the European risk and insurance management community. The 2011 survey focused on emerging risk. See "Risk Frontier Survey 2011" at http://www.commercialriskeurope.com/uploads/files/special-reports/Risk-Frontiers-Survey-2011.pdf (accessed October 16, 2012).
[112] Sclafane, S., "Advisen Spotlight: Emily Freeman on the Cutting Edge," Advisen Cyber Liability Journal, March 2012, http://corner.advisen.com/pdf_files/CLJ_Q1_2012.pdf (accessed October 15, 2012).

The data provided in this section underscore a prevalent problem in cybersecurity risk assessment due to the lack of consistent measure of historical data pertaining to cybersecurity risk and related issues.

5.1.1 Growing Cybersecurity Incidents and Costs

There is a growing number of sources providing independent assessment of cybersecurity incident trends, costs, and spending. While many sources provide a variety of cybersecurity-related information, challenges remain in limited sample sizes, the lack of consistent measures and parameters, as well as great complexity, which make it difficult to draw definite conclusions or accurately quantify the impacts of cybersecurity risks. This section presents some of the publicly-available data and analyses looking at cybersecurity risk trends in the United States. Table 3 provides a list of selected, recent surveys that were considered in this section.

Table 3. Selected Surveys on Cybersecurity Risks

Survey Title	Publication Date	Survey Conductor	Sample Type/Size
State of IT Security: Study of Utilities & Energy Companies[113] (Ponemon Energy Survey)*	April 2011	Ponemon Institute	291 IT and IT security practitioners in utilities and energy companies in the United States
Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies[114] (Ponemon Cyber Crime Survey)*	August 2011	Ponemon Institute	50 U.S. companies (including 2 from energy industry)
Chubb Survey: Concern of Cyber Risk Not Leading to Insurance Buy[115] (Chubb Survey)*	August 2012	Chubb Group of Insurance Companies	Decision-makers at 145 public companies in the United States and Canada
The Global State of Information Security Survey 2013[116] (PwC Survey)*	September 2012	PricewaterhouseCooper (PwC)	9,300 executives and IT and information security professionals from 128 countries, including 42 from energy companies and 68 from utilities in North America.

* Note: Throughout this section, references to these four surveys are made using the short name and the date of publication noted in the Table. See footnotes for full citation of each survey referenced in Table 3.

As summarized in Table 3, these surveys were conducted by different entities between 2011 and 2012 and included various types and sizes of samples or participants. The remainder of this section summarizes a few highlights of the survey results, specifically on the frequency and

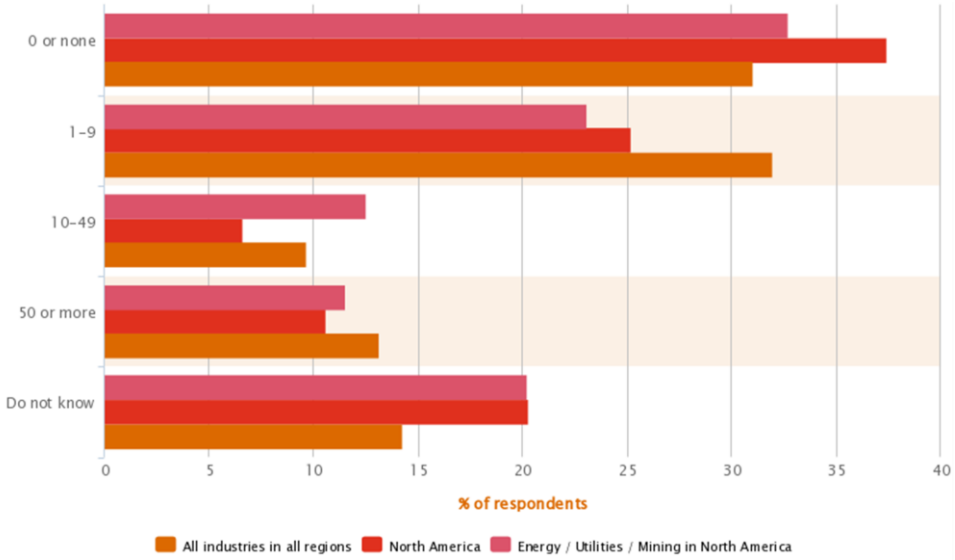
[113] "State of IT Security: Study of Utilities & Energy Companies," Ponemon Institute, April 2011, http://www.all-about-security.de/fileadmin/micropages/Krims_Krams_Pdfs/State-of-IT-Security--Study-of-Utilities-and-Energy-Companies.pdf (accessed September 19, 2012).
[114] "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies," Ponemon Institute, Sponsored by ArcSight, an HP Company, August 2011, http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf (accessed October 24, 2012).
[115] Hemenway, C. "Chubb Survey: Concern of Cyber Risk Not Leading to Insurance Buy," August 10, 2012, http://www.propertycasualty360.com/2012/08/10/chubb-survey-concern-of-cyber-risk-not-leading-to (accessed September 18, 2012).
[116] The Global State of Information, Security Survey 2013, PricewaterhouseCooper, (PwC) http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# (accessed October 23, 2012).

common sources of cybersecurity risks, as well as the impacts and costs associated with cybersecurity incidents.

Frequency and Sources of Cybersecurity Incidents

When asked to identify the frequency of cybersecurity incidents or violations in the last year, the survey participants' responses varied widely, depending on the industry, location, size, or type of the organization. In a September 2012 PwC Survey, 9,300 executives and IT professionals from all sectors participated from around the worldwide, including 40 percent or 3,720 from North America. The survey results suggested that organizations in North America experienced slightly fewer cybersecurity incidents than those in the rest of the world in the past 12 months. Approximately 55 percent of all participants said they experienced one or more cybersecurity incidents, as compared to 43 percent of North American respondents during the same period (see Figure 18).[117] Another survey received similar results from companies in North America. The August 2012 Chubb Survey of 145 public companies in the United States and Canada found that about 40 percent of the participating companies experienced a significant cybersecurity issue in a recent 12-month period.[118]

Figure 18. Number of Cybersecurity Incidents Your Organization Experienced in the Past 12 Months



Source: PwC, September 2012.

According to the September 2012 PwC Survey, energy companies experienced a slightly higher number of cybersecurity incidents compared to companies in other sectors. Among a sample of 110 energy and utility representatives from North America, 47 percent responded that they experienced one or more cybersecurity incidents, including 12 percent experiencing more than 50 incidents during a 12-month period.[119] About 20 percent of the participants, however, responded they did not know whether they experienced any cybersecurity incidents, suggesting some cybersecurity incidents could have gone unnoticed. In contrast to the PwC survey results,

[117] See PwC Survey, September 2012.
[118] See Chubb Survey, August 2011.
[119] See PwC Survey, September 2012.

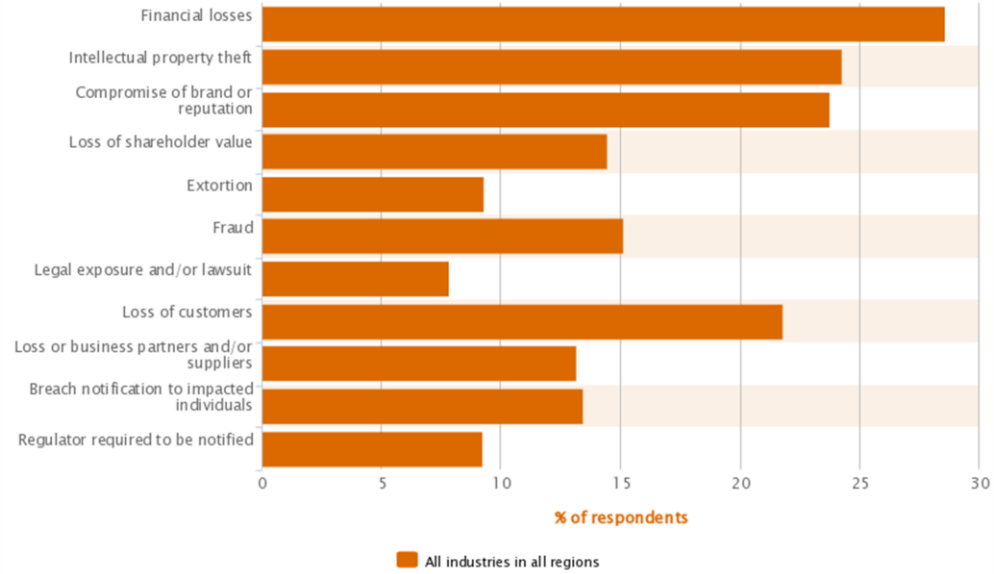
the Ponenom Institute suggested there was a much higher frequency of cybersecurity incidents in the energy industry in the United States. In Ponemon's April 2011 Survey of 291 IT security professionals at U.S. energy companies, 76 percent of the participants responded that their organization experienced one or more incidents during a recent 12-month period.[120]

In the abovementioned surveys, participants were also asked what they perceived as the main sources of cybersecurity threats. In all of the surveys, insider threats—whether malicious or negligent, or by former or current employees—were identified as one of the top cybersecurity threat sources.[121] Other key concerns included insecure Web applications, system glitches, malicious code, denial of service, stolen devices, as well as competitors and hackers.[122] In addition to these common cybersecurity threats prevalent in all industries, the energy industry faces a new set of challenges, particularly, in the implementation of smart grid technologies and systems. In the April 2011 Ponemon Energy Survey, only 16 percent of the respondents believed the existing controls in their organizations were designed to specifically protect against exploits and attacks through smart grid and smart meter-connected systems.[123] Specifically, 68 percent of the respondents expressed that they were somewhat (27 percent) or very concerned (41 percent) about the risk posed by a third party provider that is connected to the smart grid, suggesting a growing cybersecurity concern surrounding the smart grid.[124]

Impact of Cybersecurity Incidents

The cost of a cybersecurity breach is difficult to estimate, as suggested by the wide range of responses received in these surveys, because the extent of the costs related to cybersecurity

Figure 19. How was Your Organization Impacted by the Cybersecurity Incident?



Source: PwC, September 2012.

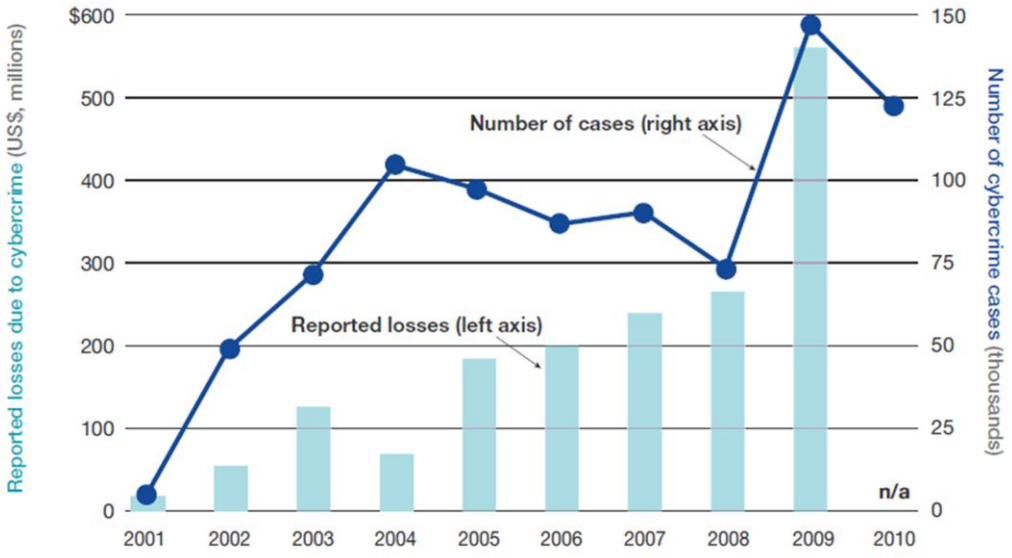
[120] See Chubb Survey, August 2012.
[121] See Ponemon Energy Survey, April 2011; Ponemon Cyber Crime Survey, August 2011; and PwC Survey, September 2012.
[122] Ibid.
[123] See Ponemon Energy Survey, April 2011.
[124] Ibid.

incidents can range from a simple infrastructure damage or financial loss to the compromise of brand reputation, loss of customers and shareholder values, as well as possible lawsuits or legal exposure (see Figure 19).[125] These types of damages to the affected organizations are not only difficult to assess, but can also take months to fully materialize. For these reasons, recent survey results revealed a wide spectrum of costs resulting from cybersecurity incidents, ranging from $156,000 to $5.5 million per event.

In the April 2011 Ponemon Energy Survey, the 291 IT security professionals at U.S. energy companies reported an extrapolated average cost of $156,000 caused by IT security incidents in a 12-month period.[126] This is a low end of estimate, however. The August 2012 Chubb Survey of 145 U.S. and Canadian companies suggested an estimated $5.5 million in organizational costs resulting from a typical data breach in 2011.[127] Similarly, the August 2011 Ponemon Cyber Crime Survey of 50 U.S. companies from all sectors reported that cybersecurity crimes cost the companies an average of $5.9 million per year, up 56 percent from the prior year.[128] A 2012 World Economic Forum report also suggested an increasing trend of cybercrime cases and economic losses due to cybercrimes in the United States. The report found that in 2009, almost 150,000 cybercrime cases were reported in the United States, resulting in more than $550 million in economic losses (see Figure 20).[129]

Due to the growing number of and costs resulting from cybersecurity incidents, utilities and energy companies are expected to increase their spending to prevent such costly cybersecurity

Figure 20. Cost and Incidence of Cybercrimes in the United States From 2001 to 2010



Note: Includes cybercrime complaints specifically referred to law enforcement.

Source: World Economic Forum, Global Risks 2012.

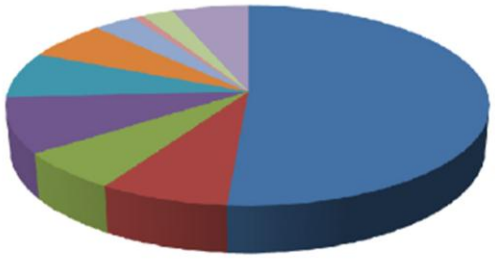
[125] PwC Survey, September 2012.
[126] See Ponemon Energy Survey, April 2011.
[127] See Chubb Survey, August 2011.
[128] See Ponemon Cyber Crime Survey, August 2011.
[129] Global Risks 2012, Seventh Edition, World Economic Forum.

events. *Bloomberg News* reported that a small sample of 21 utilities and energy companies surveyed spent an average of $45.8 million a year on computer security to prevent 69 percent of known cyber strikes against their systems in 2011.[130] Based on these responses, the report also suggested that over the next 12 to 18 months, companies would have to increase annual spending to an average of $69.3 million to be able to avert 88 percent of the attacks.[131]

Assessment of Cybersecurity Incidents by the Federal Government

In addition to the private sector, U.S. governmental organizations have implemented a variety of programs to address cybersecurity concerns. In 2003, the U.S. Department of Homeland Security (DHS), in partnership with other public and private organizations, created a Federal information security incident center called the U.S. Computer Emergency Readiness Team (US-CERT).[132] The US-CERT coordinates the response to security threats from the Internet and receives computer security incident reports from the Federal, State, and local governments, as well as commercial enterprises, U.S. citizens, and international Computer Security Incident Response Teams (CSIRTs).[133] Figure 21 provides a summary of incidents reported to US-CERT in fiscal year (FY) 2011 from all types of entities, including the Federal and State/local governments, commercial enterprises, U.S. citizens, and the CSIRTs. During FY 2011, US-CERT processed a total of 107,655 incidents, and approximately half of the reported incidents were related to phishing.[134]

Figure 21. Summary of Total Incidents Reported to US-CERT in FY 2011



Phishing	55,153	51.2%
Virus/Trojan/Worm/Logic Bomb	8,236	7.7%
Malicious Web Site	6,795	6.3%
Non Cyber	9,652	9.0%
Policy Violation	7,927	7.4%
Equipment Theft/Loss	6,635	6.2%
Suspicious Network Activity	3,527	3.3%
Attempted Access	863	0.8%
Social Engineering	2,573	2.4%
Others	6,294	5.8%
Total	**107,655**	**100.0%**

Source: White House. March 2012.

Particularly, Federal agencies have reported an increasing number of cybersecurity incidents that placed sensitive information at risk with potentially serious impacts on Federal operations, assets, and people. According to the US-CERT data, in the past six years, the number of incidents reported by Federal agencies has increased from 5,503 incidents in FY 2006 to 43,887 incidents in FY 2011, an increase of nearly 680 percent.[135]

[130] "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months," Bloomberg, February 1, 2012, http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html (accessed August 14, 2012).
[131] Ibid.
[132] U.S. Computer Emergency Readiness Team (US-CERT), http://www.us-cert.gov/ (accessed August 10, 2012).
[133] "About US-CERT," US-CERT, http://www.us-cert.gov/about-us/ (accessed August 10, 2012).
[134] "Fiscal Year 2011Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," Office of Management and Budget, March 7, 2012, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf (accessed September 28, 2012).
[135] GAO, Cybersecurity: Threats Impacting the Nation, GAO-12-666T, April 24, 2012, http://www.gao.gov/assets/600/590367.pdf (accessed August 10, 2012).

According to another US-CERT Incident Response Summary Report, there were 198 attacks on U.S. facilities with industrial control systems in 2011, a nearly fivefold increase from 2010 when only 41 incidents were reported.[136] Of the 198 attacks in 2011, 81 cyber attacks were on water supply systems, 31 on energy companies, 10 on nuclear facilities, and nine on chemical companies.[137] It is important to note that while reporting cybersecurity incidents to US-CERT is mandatory for Federal agencies and for systems operating on behalf of the Federal government, private entities' cybersecurity incident reporting to the US-CERT is done on a voluntary basis.

More information is needed to better understand the extent of cybersecurity risk since many incidents often remain unreported or under-reported. Although more cybercrime is being reported in the news than it has in the past, it is likely that the impact of cybercrimes on companies goes under-reported, as victims prefer not to disclose that their systems have been compromised.[138] While victims of the cybercrime often remain silent—often to protect their business interest and reputation—vendors of online security products have an interest in amplifying the threats of cybercrime. Further, most of the research into cybersecurity threats has been funded by those in the business of selling security services. This makes it difficult for individuals and companies to get an accurate depiction of the level of cybersecurity risk. The following section will provide an overview of cyber insurance and the challenges the insurance industry faces in managing cybersecurity risk.

> "Protecting consumers and hardening critical infrastructure do not address all cybersecurity problems. The biggest single problem is the loss of intellectual property and business information due to cyber spying. It is hard to estimate the cost of the damage but it is likely to be in the billions of dollars"
>
> - James Andrew Lewis, Center for Strategic and International Studies, September 20, 2011

5.1.2 Cyber Insurance Overview

Cyber insurance refers to a relatively new type of insurance product covering a broad range of issues relating to risk in cyberspace, with typical issues including liability, property loss, theft, data damage, and loss of income from network outages and computer failures or web-site defacement.[139] Cyber insurance may be able to enhance cybersecurity by encouraging the adoption of best practices, because insurance providers usually require a level of security or protective measures as a precondition of coverage and offer lower insurance rates to companies adopting better security measures.[140] The adaptation of best practices, in turn, would tend to encourage investments and improvements that further bolster cybersecurity.

In general, most businesses purchase a package of insurance policies called the business owners policy, which typically includes the following: (1) property insurance for buildings and contents;

[136] "ICS-CERT Incident Response Summary Report," June 2012, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf (accessed September 13, 2012).
[137] Ibid.
[138] Ibid.
[139] "Incentives and barriers of the cyber insurance market in Europe," European Network and Information Security Agency, June 28, 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport (accessed September 13, 2012).
[140] "Cyber-Insurance Metrics and Impact on Cyber-Security," Internet Security Alliance, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf (accessed September 19, 2012).

(2) business interruption insurance, which covers the loss of income resulting from a fire or other catastrophe that disrupts the operation of the business; and (3) liability protection, which covers a company's legal responsibility for the harm it may cause to others.[141] However, none of these policies covers data breaches or anything data-related, due to what is known as the "intangible property exclusion."[142] Despite this, a majority of businesses still do not have a cybersecurity policy, as suggested in recent surveys.

According to the August 2012 Chubb Survey (see Table 3), while 71 percent of the companies surveyed had an incident response plan for an electronic security breach, 57 percent of them did not have cyber liability insurance as part of their plan.[143] Another study, "the Risk and Finance Manager Survey" conducted by Towers Watson in April 2012 found that 72 percent of the 153 companies surveyed did not purchase network security/privacy liability policies.[144] The survey further examined that even those companies that purchased cyber insurance needed to ensure that they have purchased adequate coverage. The survey showed 43 percent of the respondents purchased cyber insurance policies with a $1 million to $5 million limit;[145] however, a serious cybersecurity incident could cost exponentially more. For example, Heartland Payment Systems announced the discovery of a criminal breach of its payment systems in January 2009. Although the company had insurance coverage, an estimated $115.9 million was left uncovered after the insurance policy paid $31.2 million through the end of 2011, according to corporate filings in February 2012.[146]

Cyber insurance is so new that a typical or standard policy does not exist.[147] In general, insurance policies are divided into first party and third party policies; cyber insurance policy contains both types of coverage. First-party losses refer to direct losses sustained by the insured through cyber-related activities, including data destruction, theft, hacking, viruses, extortions, and programming errors. Third-party losses concern a company's liability to losses sustained by third parties caused by the insured's cybersecurity incident.[148] Thus, the third-party losses refer to the claim made by a third party against the insured seeking relief against damages caused by an "error, or omission" or "wrongful act" done by the insured.[149] Although these key characteristics describe the "typical" components of the cyber insurance, cybersecurity risk is such a broad area that any

[141] "What Does a Businessowners Policy (BOP) Cover?," Insurance Information Institute, http://www.iii.org/articles/what-does-a-businessowners-policy-cover.html (accessed October 23, 2012).
[142] Harrison, J.D., "Cybersecurity insurance: What small businesses need to know," *Washington Post*, December 28, 201, http://www.washingtonpost.com/blogs/on-small-business/post/cybersecurity-insurance-what-small-businesses-need-to-know/2011/12/28/gIQAYlL5MP_blog.html (accessed October 8, 2012).
[143] Ibid.
[144] "2012 Risk and Finance Manager Survey," Towers Watson, April 2012, http://www.towerswatson.com/assets/pdf/6842/2012-Risk-and-Finance-Manager-Survey-PDF.pdf (accessed October 8, 2012).
[145] Ibid.
[146] King, R., "As Flame Spreads, Most Companies Lack Cybersecurity Coverage," *Wall Street Journal*, May 29, 2012, http://blogs.wsj.com/cio/2012/05/29/as-flame-spreads-most-companies-lack-cybersecurity-coverage/ (accessed October 8, 2012).
[147] Sagalow, Ty R., The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce, and cyber perils, Reactions Publishing Group, Ltd., London, United Kingdom, 2002.
[148] "Cyber risks: Understanding your insurance protection," Marsh, April 2011, http://usa.marsh.com/Portals/9/Documents/UnderstandingCyberRisks2011.pdf (accessed September 19, 2012).
[149] Sagalow, Ty R.,2002.

insurance policy has to be tailored to the specific risks facing each organization. Consequently, the few insurance products first introduced to market have been highly customized.[150]

5.1.3 Cyber Insurance Market Trends and Challenges

Several sources have suggested that cyber insurance is a growing market. The estimated U.S. cyber insurance market size varies widely, ranging from $600 million as reported by Lloyd's in November 2011[151] to $1 billion in annual gross written premium as suggested by the Betterley Report in June 2011.[152] Another source, Strategic Risk, estimated the size of cyber insurance market to be about €620 million or $800 million, and that there were 30 to 40 carriers offering cyber-insurance products in the United States in 2012.[153] Given the estimated $1.7 trillion U.S. insurance premium market in 2011,[154] these numbers suggest that the current cyber insurance market is less than one percent of the overall insurance market in the United States. Despite the small share of cyber insurance in the overall insurance market place, the U.S. cyber insurance market is considered relatively mature compared to other nations, according to the European Network and Information Security Agency.[155]

The U.S cyber insurance market is expected to grow further in the near future, partially due to recent Federal guidelines issued by the U.S. Security and Exchange Commission (SEC). In October 2011, the SEC released a new guidance requiring that public companies disclose "material" cyber attacks and their costs to shareholders. The guidance specifically requires companies to disclose a "description of relevant insurance coverage."[156] In the coming years, more companies are expected to buy cyber insurance policies because of new SEC requirements, according to experts.[157]

Cybersecurity risk is a complex, growing threat in today's business environment, including the Energy Sector. However, as is common with emerging risks, creating new insurance products for

[150] "Emerging Risks 2012," Allianz, April 2012, http://www.agcs.allianz.com/assets/Global%20offices%20assets/UK/Documents/EMERGING%20RISKS%20REPORT%202012_low%20res.pdf (accessed September 13, 2012).
[151] Palmer, M. "Insurance: The trade-off between risk and cost," *Financial Times*, November 1, 2011, http://www.ft.com/cms/s/0/9d4045a6-f8a1-11e0-ad8f-00144feab49a.html#axzz26NQoasuu (accessed September 13, 2012).
[152] The Betterley Report, Cyber/Privacy Insurance Market Survey—2012: Surprisingly Competitive, as Carriers Seek Market Share, August 2012, http://betterley.com/samples/cpims12_nt.pdf (accessed September 17, 2012).
[153] "Evolving cyber cover," Strategic Risk, March 2012, http://www.strategic-risk.eu/Journals/2012/02/22/i/j/w/RiskFinancing_Mar12.pdf (accessed September 17, 2012).
[154] Nordman, E. C., National Association of Insurance Commissioners, 2010.
[155] "Incentives and barriers of the cyber insurance market in Europe," European Network and Information Security Agency, June 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport (accessed September 17, 2012).
[156] "CF Disclosure Guidance: Topic No. 2—Cybersecurity," Division of Corporation Finance Securities and Exchange Commission, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed October 18, 2012).
[157] Perlroth, N., "Insurance Against Cyber Attacks Expected to Boom," *New York Times*, December 23, 2011, http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ (accessed October 18, 2012).

cybersecurity risk requires a complex actuarial approach that can take a long time.[158] Especially for the critical infrastructure assets and systems, underwriting some of the cyber exposures is a difficult task, as they pertain to not only the physical buildings and properties, but also critical engineering, production, distribution, and emergency systems.[159]

Currently, the insurance industry may not have the capacity to deal with this issue, as there remain a number of open questions about how one can quantify and underwrite some of these exposures. The threats to systems supporting critical infrastructure are evolving and growing; however, reliable indicators of measuring the frequency or the economic impact of cyber attacks are rarely available. Thus, protecting and insuring these many components of critical infrastructure is a challenging, ongoing task for the insurance industry, as well as for the policymakers who are seeking approaches to protect critical infrastructure in the face of cyber threats. To be insurable, a risk must meet the four basic requirements for insurability; cybersecurity risk violates each of the four requirements as specified in Table 4.[160]

Table 4. Traditional Requirements for Insurability and Possible Violation of Insurability in Cybersecurity Risk

Requirement	Definition	Violation
Estimated Frequency	• Insurance requires a large number of observations to develop predictive rate-making models (an actuarial concept known as credibility).	• Very few data points exist. • Cyber insurance modeling is still in infancy and untested. • Threat assessments remain inconsistent.
Estimated Severity	• Maximum possible/probable loss must be at least estimable in order to minimize "risk of ruin" (insurer cannot run an unreasonable risk of insolvency though assumption of the risk).	• Potential loss is virtually unbounded. • Losses can easily exceed insurer capital resources for paying claims.
Diversifiable Risk	• "Law of Large Numbers" helps make losses manageable and less volatile. • Must be able to spread/distribute risk across a large number of risks.	• Losses are likely highly-concentrated geographically or by industry (e.g., the World Trade Center, power plants).
Random Loss Distribution/ Fortuity	• Events are individually unpredictable in terms of time, location, and magnitude. • Probability of loss occurring must be purely random and fortuitous.	• Cyber attacks are planned, coordinated and deliberate acts of destruction. • Targets can dynamically shift from "hardened targets" to "soft targets." • Intruders can adjust tactics to circumvent new security measures. • Actions of U.S. and foreign governments may affect likelihood of cybersecurity incidents.

Source: Insurance Information Institute, September 2012. See Footnote 160.

[158] "Risk Frontier Survey 2011," Commercial Risk Europe, http://www.commercialriskeurope.com/uploads/files/special-reports/Risk-Frontiers-Survey-2011.pdf (accessed October 18, 2012).
[159] Sclafane, S., "Advisen Spotlight: Emily Freeman on the Cutting Edge," Advisen Cyber Liability Journal, March 2012, http://corner.advisen.com/pdf_files/CLJ_Q1_2012.pdf (accessed October 15, 2012).
[160] Testimony of Robert P. Hartwig, Ph.D., CPCU, President & Economist, Insurance Information Institute, before the House Committee on Financial Services, Subcommittee on Insurance, Housing and Community Opportunity , "TRIA at Ten Years: The Future of the Terrorism Risk Insurance Program," September 11, 2012, Washington, D.C., http://financialservices.house.gov/uploadedfiles/hhrg-112-ba04-wstate-rhartwig-20120911.pdf (accessed October 30, 2012).

In addition to the failure to meet these traditional requirements for insurability, emerging risks—including cybersecurity and space weather risks—face several common obstacles. Following an overview of space weather risks in the next section, the challenges in managing emerging risks through insurance, as well as the four fundamental requirements for insurability are further discussed in Section 5.3.

5.2 Space Weather Risks

Space weather events refer to disturbances that occur in space that have the potential to disrupt modern technologies and infrastructure. Space weather events, similar to ordinary natural weather events, can vary widely in severity and in their potential impacts on critical infrastructure. Even more than natural hazards, space weather events are characterized by considerable uncertainty about potential duration and consequences of, as well as recovery from, the event. Thus it is one of the most difficult-to-quantify risks that could cause a significant loss and disruption to critical infrastructure in space and on the earth. The risks posed by space weather are increasing due to the growing interconnected systems and infrastructure that businesses and other activities rely on. Modern businesses often depend on other businesses to supply both raw materials and a wide range of services, such as in the energy supply and distribution services. A space weather event could potentially have a wide regional or even global impact by triggering cascading failures across multiple infrastructure and systems.

Recognizing the potential vulnerabilities of critical infrastructure to the emerging space weather risk, numerous organizations throughout the world have been studying this issue. In the United States, the Federal government coordinates space weather responsibilities through the U.S. National Space Weather Program (NSWP), a program in which eight agencies participate, including the National Aeronautics and Space Administration, the U.S. Department of Commerce's National Oceanic and Atmospheric Administration (NOAA), the National Science Foundation, and the U.S. Departments of Defense, Energy, Interior, State, and Transportation.[161] NOAA's Space Weather Prediction Center is the single point of responsibility for monitoring and reporting on space weather activities for the civil and commercial communities.[162] NOAA's Space Weather Scale rates solar activities based on severity levels from 1 (minor) to 5 (extreme), including geomagnetic storms, solar radiations, and radio blackouts.[163]

In addition, the U.S. Departments of Defense, Energy, and Homeland Security, as well as the NERC have conducted numerous studies and exercises concerning the effects of geomagnetic storms on critical energy infrastructure and created various programs to develop mitigation measures against their potential effects.

Such an emerging risk can create a new, potential market for insurance products, and major global reinsurance companies, such as Allianz, Lloyd's, Swiss Re, and Zurich have researched, investigated, and presented their findings about the effects of space weather on various

[161] "Severe Space Weather Events—Understanding Societal and Economic Impacts, A Workshop Report," National Research Council of the National Academies, 2008, http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf (accessed October 31, 2012).
[162] Space Weather Prediction Center, NOAA, http://www.swpc.noaa.gov/ (accessed September 20, 2012).
[163] Ibid.

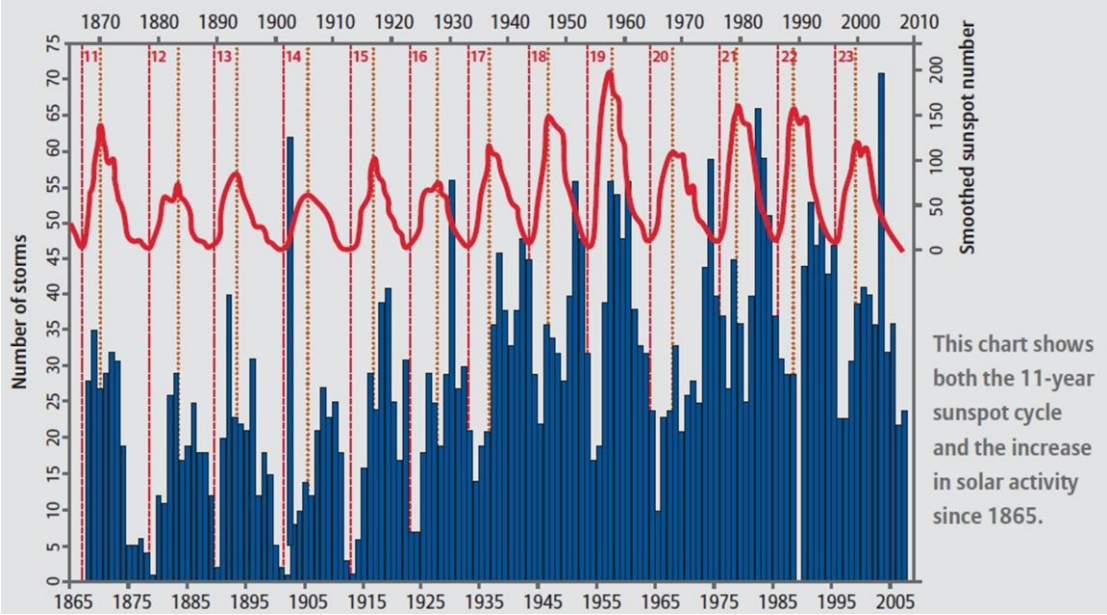
infrastructure and systems.[164] The remainder of this section summarizes some of the key findings on solar weather risk provided by the abovementioned reinsurance sources.

5.2.1. Fundamentals of Space Weather

"Space weather" is a phenomenon caused by radiation and atomic particles emitted by the sun and the stars.[165] The sun is the primary source of space weather; its core continuously undergoes nuclear fusion, emitting electromagnetic radiation and charged particles.[166] During a solar storm, coronal mass ejections, or high-speed bursts of dense electromagnetic radiations, are released toward the earth. This intensifies electric currents that flow in the upper atmosphere of the earth, causing rapid changes in earth's magnetic field.

The intensity of space weather events is influenced by an 11-year cycle of solar activity as illustrated in Figure 22. This is traditionally measured by counting the number of sunspots, or dark spots on the face of the sun that appear dark. At the height of a solar cycle, violent events occur on the sun that causes the sun to eject solar matter and energy towards the earth. During the minimum of the cycle, the sun remains quieter. As shown in Figure 22, solar activities have gradual increased since 1865. In 2008, the solar cycle hit a low point, indicating the next peak

Figure 22. Sunspot Cycle and Annual Number of Magnetic Storms



Source: Allianz, based on British Geological Survey, http://www.agcs.allianz.com/assets/PDFs/GRD/GRD%20individual%20articles/GRD-2009-01-SpaceWeather.pdf.

[164] Allianz: "Space Risks: A new generation of challenges," August 2012, http://www.agcs.allianz.com/assets/PDFs/white%20papers/1844%20Allianz%20Space%20White%20Paper%201o.pdf; Lloyd's: "Space Weather: Its Impact on Earth and implications for business," November 2010, http://www.lloyds.com/~/media/Lloyds/Reports/360/360%20Space%20Weather/7311_Lloyds_360_Space%20Weather_03.pdf; Swiss Re: "Space weather: Hazard to the Earth?," 2000, http://media.swissre.com/documents/pub_space_weather_en.pdf; Zurich: "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" April 8, 2010, http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/media/solarstorms.pdf.

[165] "Space Weather, Hazard to the Earth?" Swiss Re, 2000.

[166] Ibid.

would be occurring around 2011 and 2012; however, the start of the current solar maximum has been delayed by two years and is expected to occur sometime between 2013 and 2014.[167]

Potential Impacts of Space Weather on Critical Infrastructure

Geomagnetic storms, which affect the planet's magnetic field, have the potential to cause a considerable damage across the globe with a single event.[168] The impact of solar storms on space and aviation industries can be significant, with potential effects ranging from damage and malfunctioning of satellites to that of possible long-term radiation effects on interplanetary flights.[169] That is because an extreme solar storm cycle activity produces solar electromagnetic and particle radiation which can affect the operation of various infrastructure and systems. These solar energetic particles can impact critical communications and global positioning systems (GPS), airline navigation and operations, electric power systems, telecommunications, the Internet, railway installations, and oil and natural gas pipelines. Particularly, as a solar storm approaches the earth, fluctuations in earth's magnetic field cause geomagnetically-induced currents (GICs) in transmission lines and other conducting elements like pipelines.

Electric Power Transmission Grid and Transformers

Although not fully understood, there has been a significant amount of research on the effects that GICs could have on transformers and high-voltage power lines. Some of the possible transmission line-related risk factors may include directional orientation of transmission grid lines (east/west or north/south), their lengths, and conductor resistance. Power infrastructure located in northern latitudes (e.g., United States and Canada) is more likely to experience GICs due to the infrastructure's physical proximity to earth's magnetic north pole.[170] Additional risk factors of a transformer include its function, age, position, type, design, windings, and grounding.[171]

GICs cause voltage differences between transmission lines, and these voltage differences induce direct currents in addition to the normal alternating currents, which can result in transformer saturation and possible overheating, shutdown, or even destruction of the equipment.[172] A large portion of the current carried by a saturated transformer is reactive, and this reactive current can reduce the transmitting capacity of the system, causing a system failure or, in extreme cases, a complete blackout.[173] The solar weather event that occurred in Quebec in March 1989 provides

[167] "Solar Weather: Its impact on Earth and implications for business," Lloyd's, 2010.
[168] "Risk Management Issue Brief: Geomagnetic Storms: An Evaluation of Risks and Risk Assessments," the Office of Risk Management and Analysis, U.S. Department of Homeland Security, May 2011, http://www.dhs.gov/xlibrary/assets/rma-geomagnetic-storms.pdf (accessed August 16, 2012).
[169] Riswadkar, A.V. and Dobbins, B., "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side'," Zurich Services Corporation, April 8, 2010, http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/media/solarstorms.pdf (accessed September 20, 2012).
[170] Kappenman, John G., et al., "Solar Wind Monitor Satellite Crucial for Geomagnetic Storm Warning," IEEC Power Engineering Review, 1990.
[171] "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" Zurich, 2010.
[172] Ibid.
[173] "Space Weather, Hazard to the Earth?" Swiss Re, 2000.

some insight into the potential impacts a geomagnetic disturbance could have on the electrical grid system as summarized next.[174]

The 1989 Solar Storm in Quebec
A severe solar event occurred in Quebec, Canada on March 13, 1989, damaging several transformers on the Hydro Quebec system and resulting in a cascading effect that shut down the entire Quebec power grid system in 90 seconds. The blackout lasted about nine hours, leaving approximately five million people without power. An estimated cost of $2 billion Canadian dollar incurred during the event, including C$13 million of direct damage to the Quebec power grid. This event also caused problems in power systems elsewhere, including a permanent damage to a $12 million transformer in New Jersey as well as major damage to two large power transformers in the United Kingdom.

Sources: Zurich and Lloyd's, 2010.

While historic space weather events such as the 1989 Quebec event provide a glimpse into the effects of solar events, several factors have changed in a way that could exacerbate the potential impacts of similar scale of events today. These changes include the aging U.S. power infrastructure, including large power transformers (LPTs), which could increase vulnerability to adverse events.[175] Supply and procurement of LPTs could present a challenge, as it can take more than 12 months to replace and LPT, due to its long and complex procurement process.[176] Currently, the United States heavily depends on oversea manufacturers for its demand for LPT. In 2011, the United States imported approximately 85 percent of its LPTs with a capacity rating greater than or equal to 60 mega volt ampere (MVA).[177]

The interconnected nature of the U.S. electric grid and the cascading effects of GICs are a serious vulnerability, presenting a challenge for protection and emergency response measures. Compared to the effects of natural hazards on the electric power grid, space weather-related damages and disruption to the power grid have the potential to leave a broad footprint across a large region for an extended period.[178]

The society has never had such technological dependence during an extreme solar event as it does today. The United States depends on various technologies—electricity, satellite, GPS, telecommunications, and the Internet—that are interdependent of one other for many essential functions, which could further heighten the impact of a solar event. Such a wide-ranging and long-lasting power outage has the potential to bring a cascading societal and economic impact that is difficult to quantify. That is because a geomagnetic storm that degrades the electric power

[174] "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" Zurich, 2010; "Solar Weather: Its impact on Earth and implications for business," Lloyd's, 2010.
[175] For more information about issues surrounding large power transformers procurement and supply issues, see "Large Power Transformers and the U.S. Electric Grid," U.S. Department of Energy, June 2012, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf (accessed October 30, 2012).
[176] Ibid.
[177] Ibid.
[178] "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" Zurich, 2010.

grid would affect not only the Energy Sector but the transportation, communications, banking, and finance sectors, as well as government services and emergency response capabilities.

Oil and Natural Gas Pipelines

GICs flow in any large metallic structure or systems, such as bridges or rail networks, in a similar manner as in pipelines, power transmission lines, and telecommunication cables. However, none of these systems has yet been sufficiently investigated with regard to the possible effects of GICs. In case of oil and natural gas pipelines, GICs pose no acute risk for catastrophic failure; however, GICs may cause corrosion or problems in corrosion monitoring because pipelines have a tendency to corrode when an electric current flows from the metal into the ground. The intensity of GICs along a pipeline and the voltage differences between pipeline and ground are dependent on the geophysical situation and the details of the pipeline network.[179] Additional factors affecting the degree of risk include pipeline construction, such as the material, diameter, bends, branches, insulated flanges, and integrity of insulated materials.[180]

5.2.2 Mitigation Measures and Recent Developments

The risk of extreme solar weather is not a totally new or unknown emerging risk; however, current level of understanding is based on prior events in the last 20 to 30 years, including the 1989 Quebec blackout event. While scientists know a lot about the possible causes and effects of solar weather from previous cycles, the economic impact that could result from a solar event is far less certain. That is because recent developments—the increased dependence on technology and the close interdependency of global economy—have produced two risk-augmenting factors: the number of systems likely to fail has increased considerably and may result in accumulation of losses, and the growing interaction and interdependencies may further amplify the effect of a solar event.[181] This increased risk has induced numerous activities to enhance protection of the U.S. electric grid against solar events.

The U.S. government and the electric power industry have been working to enhance protection against space events. For example, since the 1989 solar event, Hydro Quebec reportedly has installed transmission-line series capacitors at a cost of more than $1.2 billion and has improved its various operational mitigation strategies, according to Zurich.[182] However, most utilities do not have spare LPTs, which can cost more than $10 million per unit and take more than a year to manufacture.

Recognizing the challenges utilities face in procuring this expensive, large power equipment, the U.S. government collaborated with the private sector to develop a possible relief to this issue. The DHS Science and Technology Directorate, along with their partners, the Electric Power Research Institute, ABB, and CenterPoint Energy (CNP), and the support of DOE and DHS Office Infrastructure Protection, have developed a prototype extra high voltage (EHV) transformer that will drastically reduce the recovery time associated with EHV transformer issues. The Recovery Transformer is a 345:138kV, 200 MVA per phase transformer (equivalent to 600MVA), designed to be an applicable replacement for more than 90 percent of transformers in this voltage class. The Recovery Transformer is also lighter, smaller, and easier to transport

[179] "Space Weather, Hazard to the Earth?" Swiss Re, 2000.
[180] "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" Zurich, 2010.
[181] "Space Weather: Hazard to the Earth?" Swiss Re, 2000.
[182] "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side,'" Zurich, 2010.

and quicker to install than a traditional EHV transformer. The prototype transformer delivery and set up was successfully demonstrated in March 2012 and is currently operating in CNP's grid for a one-year monitoring period.

In addition, the NERC, as the designated electrical reliability organization, formed the Geomagnetic Disturbance Task Force (GMDTF) in 2010. Through this task force, NERC has been collaborating with the government and the industry to address the implications of severe GMD events on the electric power grid. In 2012, NERC released a special assessment, "2012 Special Reliability Assessment: Effects of Geomagnetic Disturbances on the Bulk Power System," which provided a comprehensive look at multiple, complex issues to evaluate GMD effects.[183] During 2012, NERC has been implementing the Spare Equipment Database Program, which will help determine the extent to which spare transformers are available across North America.

Most recently, on October 24, 2012, the U.S. Federal Energy Regulatory Commission (FERC) issued a Notice of Proposed Rulemaking, directing the NERC to develop Reliability Standards that address the impact of GMD on the reliable operation of the Bulk-Power System. The Reliability Standards would require owners and operators to "develop and implement a plan so that instability, uncontrolled separation, or cascading failures of the Bulk-Power System . . . will not occur as a result of a GMD."[184]

5.2.3 Insurance for Space Weather

Insurance industry provides information and raises awareness about emerging risks, and it is the responsibility of the insured to implement risk-mitigating measures.
The insurance industry, as one of the key risk bearers of space weather risks, has high interest in mitigating these risks by encouraging improved technological prevention and safety standards, as well as engaging in supporting businesses and clients in tackling space weather risks.[185] For these reasons, early warning systems capable of accurately and timely detecting solar activities and space weather storms are important.

Businesses that are heavily dependent on utility services, including the supply of electricity, commonly purchase what is known as the "Service or Utility Interruption Coverage"; however, it is unclear whether this type of insurance product includes protection against space weather events.[186] Typically, property damage or business interruption insurance policy is restricted to physical damage. However, based on some case laws, it is possible that space weather events and their effects on the power grids and global positioning satellites are covered under a "loss of

[183] "2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System," NERC, February 2012, http://www.nerc.com/files/2012GMD.pdf (accessed September 20, 2012).
[184] "Reliability Standards for Geomagnetic Disturbances," Notice of Proposed Rulemaking, Federal Register, Docket No. RM12-22-000, October 24, 2012, https://www.federalregister.gov/articles/2012/10/24/2012-26131/reliability-standards-for-geomagnetic-disturbances (accessed October 24, 2012).
[185] "Space Weather Risks from an Insurance perspective," Munich Re, 2011.
[186] Claverol, M., "Space Weather- The Peril of The Future? Understanding Business Interruption Claims," Property Insurance Coverage Law Blog, September 23, 2012, http://www.propertyinsurancecoveragelaw.com/2012/09/articles/commercial-insurance-claims/space-weather-the-peril-of-the-future-understanding-business-interruption-claims/ (accessed October 31, 2012).

functionality" theory if a policy does not specifically define the term "physical loss or damage" in the insurance policy terms.[187]

The widening, potential impact of solar events in today's society presents a variety of new elements that may ultimately affect the insurance industry through personal injury, property, and financial losses. While the basic premise of insurance, namely of distributing the losses suffered by individual policyholders over all policyholders, still remains, the irregular nature of space weather raises questions about the integrated risk structure.[188] This irregularity means that the probability and extent of losses that may be incurred by the various parties involved in space and air travel, electric power generation and transmission, telecommunications, or oil and gas transport, are not necessarily comparable. Therefore, individual risk assessment must be performed for each insured person or company, so that premiums appropriate for the risk may be determined and charged.[189] The predictability aspect is important to consider because insurance coverage is generally restricted to sudden and accidental events.

As of 2000, there were 20 insurers worldwide offering what is called "satellites insurance,"[190] which covers three risks: (1) the re-launching of the satellite if the launch operation fails; (2) replacing the satellite if it is destroyed, positioned in an improper orbit, or fails in orbit; and (3) liability for damage to third parties caused by the satellite or the launch vehicle.[191] The U.S. Department of Defense estimated that solar disruptions to government satellites cost about $100 million a year. According to an analysis, satellite insurers paid out nearly $2 billion between 1996 and 2005 to cover commercial satellite damages and losses, some of which were precipitated by adverse space weather.[192] However, these estimates did not include the impacts of space weather events on other critical infrastructure, including power transformers. According to a 2008 report by the NAS, the United States is not prepared to cope with the effects of what is called a "space weather Katrina." According to a NAS report, potential permanent damage to power transformers and other electrical systems caused by a severe geomagnetic storm scenario could cost up to $2 trillion to repair and take up to 10 years for a full recovery.[193] This conclusion, however, has been criticized for its assumptions and methodology and does not represent a consensus of technical experts in the utility or transformer manufacturing industries; the potential impact described could be thought of as a speculative worst-case scenario.

[187] Ibid; In Wakefern Food Corp (Shop Rite) v. Liberty Mutual Fire Ins. Co., 406 N.J. Super 524 (Sup. Ct. N.J. 2009) the court interpreted a standard Utility Service Interruption form in the context of a four-day power outage, not caused by space weather, but a cascade power grid failure that affected millions in North America.
[188] "Space Weather, Hazard to the Earth?" Swiss Re, 2000.
[189] Ibid.
[190] Gould, A.J., Linden, O.M., "Estimating Satellite Insurance Liabilities," Casualty Actuarial Society, 2000, http://www.casact.org/pubs/forum/00fforum/00ff047.pdf (accessed November 5, 2012)
[191] Ibid.
[192] Odenwald, S. and Green, J. "Bracing the Satellite Infrastructure for a Solar Superstorm," Scientific American, July 28, 2008, http://www.scientificamerican.com/article.cfm?id=bracing-for-a-solar-superstorm&page=5 (accessed September 21, 2012).
[193] Koebler, J., "Experts: Extreme Solar Storm Could Cause Cosmic 'Katrina'," U.S. News, March 5, 2012, http://www.usnews.com/news/articles/2012/03/05/experts-extreme-solar-storm-could-cause-cosmic-katrina (accessed September 20, 2012).

5.3 Challenges in Insuring Critical Infrastructure from Emerging Risks

As in the case of cybersecurity and space weather, managing emerging risks is a challenge for both policymakers as well as owners and operators, particularly due to the general lack of understanding and historical data pertaining to the impacts associated with those risks. In addition to the lack of supportive information, the insurability—or transferring of risk to the insurance industry—of many emerging risks is often questionable.

The following four criteria must be met for an event or risk to be insurable:[194]

- Randomness: The time and location of an insured event must be unpredictable and the occurrence itself must be independent of the will of the insured (i.e. accidental).
- Assessability: The frequency that an event will occur and the severity of the resulting damage can be estimated and quantified within reasonable confidence limits.
- Mutuality: A sufficient number of endangered parties must join together to build a risk pool in which risk is shared and diversified at economically fair terms.
- Economic viability: Insurers must be able to charge a premium that corresponds to the underlying risk including capital costs and expenses.

In addition to falling short of meeting the traditional requirements for insurability, a number of obstacles remain concerning emerging risks, including the following:[195]

- The general public's low level of familiarity with emerging risks;
- Uncertainty about what risks are being insured;
- The fluctuation in risks and threats driven by technology advancement;
- Lack of adequate reinsurance or government's intervention as the "insurer of last resort";
- The risk of a global catastrophic event, resulting in overwhelming number and costs of claims;
- The misconception by the insured that existing insurance products or self-insurance are sufficient to cover the risks; and
- The price volatility of insurance products due to the nature of evolving threats and the uncertainty in the potential effects of emerging risks.

Developing insurance mechanisms for protecting critical infrastructure from emerging risks remains a significant challenge. The Energy Sector continues to progress in advanced technology solutions, including wireless control and data transfer applications. Such a wireless application may enable a faster, more efficient recovery from a disaster; however, it may also increase the vulnerability of the system, because wireless technologies are more susceptible to space weather events and cyber attacks than the traditional wired systems. With increased interdependencies across various critical infrastructure sectors and systems, as well as the growing dependence of the society on critical infrastructure and advanced technologies to function, the question of insurability faces a new set of challenges in critical infrastructure protection. Routine

[194] "Power Blackout Risks: Risk Management Options," CRO Forum, November 2011, http://www.thecroforum.org/assets/files/publications/CRO-Position%20Paper%20-%20Power%20Blackout%20Risks-.pdf (accessed November 1, 2012).

[195] "Incentives and barriers of the cyber insurance market in Europe," European Network and Information Security Agency, June 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport (accessed September 17, 2012).

government involvement in numerous existing catastrophic risk coverage programs (e.g., floods, hurricanes, earthquakes, and terrorism) may be an implicit recognition that the public sector's engagement may be necessary to develop and ensure certain insurance programs.[196]

VI. Concluding Thoughts

In this study, DOE OE discussed key traditional and emerging risks affecting the Energy Sector as perceived by the insurance industry. Energy infrastructure and systems are widely-diverse and geographically-dispersed assets, and man-made and natural hazards can cause a considerable damage to this critical infrastructure. In addition to natural disasters, which traditionally have been a key focus of the energy industry, the critical infrastructure community is confronting new, emerging risks such as cybersecurity and space weather events. Therefore, this report examined the ways in which the insurance industry perceives and manages risks, including the identification and assessment of risks, as well as the methodologies to quantify and measure their potential impacts. Particularly, the paper presented key emerging risks in the Energy Sector and the challenges the insurance industry faces in offering financial risk management instruments for such risks.

Insurance as a Risk Management Option

- Insurance mechanisms can be a useful tool for energy infrastructure owners to mitigate risk and reduce financial impact by encouraging investments in security and mitigation measures that can help enhance resilience, which can then induce reduced insurance rates.
- With an abundance of historical data on natural disasters, including their economic impacts, the insurance industry has developed and maintained technical and actuarial expertise for providing risk assessments and risk allocation mechanisms. However, there exists no universal/standardized methodology to measure or quantify the impacts of natural hazards.
- The cost of natural disasters has increased considerably in the United States for both insured and uninsured in the past few decades, and meteorological events—storms and hurricanes—historically have caused the most economic damage.
- The United States has a mature and very large insurance industry—$1.7 trillion or a third of the world insurance market—that offers a wide range of insurance products; however, less than one percent of this is attributed to the cyber insurance market.
- A large portion of the U.S. population, businesses, and critical infrastructure may currently be underinsured, especially considering the recent observation of growing climate variability and impacts of natural disasters.
- Public insurance, while sometimes necessary, has a few problems. Specifically, some public insurance programs may be offering affordable insurance premiums that neither accurately reflect price signals of risks nor garner sufficient funds necessary to fund the recovery from a disaster.

[196] Auerswald, P., et. al.. "The Challenge of Protecting Critical Infrastructure" Center for Risk Management and Decision Processes – The Wharton School of the University of Pennsylvania, October 2005, http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf (accessed November 6, 2012).

Challenges in Protecting against Emerging Risks

- Emerging risks in the Energy Sector present a particular problem. Cybersecurity risk is seen as a rapidly growing and evolving threat against critical infrastructure, including that of the Energy Sector. While there are a growing number of sources that attempt to measure or quantify the threat and consequences of cybersecurity risk, currently-available data are inadequate to accurately assess the risk and develop proper insurance products.
- The lack of historical, quantitative data pertaining to emerging risks—both cybersecurity and space weather—does not meet the basic requirements of insurability, particularly:
    - Assessability, or the ability to estimate the severity and frequency of the event; and
    - Economic viability, or the ability to charge the premium that accurately reflects the actual underlying risk including capital costs.
- In addition, both cybersecurity and space weather events fail to meet the "randomness" condition of insurability because:
    - Cyber attacks are planned ahead and carefully targeted in highly-concentrated geographical areas or in certain industries (e.g., power plants); however, the method and effectiveness of these attacks are uncertain, as are to the potential mitigation options against such evolving threats; and
    - For space weather events, the timing of the event and the geographical locations that are mostly likely to be affected by solar storms can be predicted albeit not with great accuracy at present.
- Other challenges in developing insurance instruments for emerging risks include:
    - The general public's low level of familiarity with emerging risks;
    - The fluctuation in risks and threats driven by technology advancement, as well as changing mitigation, restoration, and recovery approaches;
    - The risk of a regional, national, or global catastrophic event, resulting in overwhelming number and cost of claims;
    - The lack of adequate reinsurance or government's intervention as the "insurer of last resort"; and
    - The misconception by the insured that existing insurance products or self-insurance are sufficient to cover emerging risks; and
    - The price volatility of insurance products due to the nature of evolving threats and the uncertainty in the potential effects of emerging risks.

While insurance instruments can be a useful risk mitigation tool for critical infrastructure by encouraging resilience-enhancing investments and facilitating recovery after a disaster, they also face a number of complex challenges as highlighted in this report. The public sector's engagement may be necessary to develop and maintain some insurance programs (e.g., flood, terrorism); however, the respective roles and responsibilities of public and private partners in providing adequate protection of critical infrastructure against certain risks—including cybersecurity and space weather events—through insurance remain unclear.

Appendix A. Acronyms

CNP	CenterPoint Energy
CRO	Chief Risk Officers
CSIRTs	Computer Security Incident Response Teams
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EIA	U.S. Energy Information Administration
EHV	Extra high voltage
Entergy	Entergy Corporation
ESF	Emergency Support Function
FCIC	Federal Crop Insurance Corporation
FEMA	Federal Emergency Management Agency
FERC	U.S. Federal Energy Regulatory Commission
FIRM	Flood insurance rate maps
FTIP	Federal Terrorism Insurance Program
FY	Fiscal year
GAO	U.S. Government Accountability Office
GIC	Geomagnetically-induced current
GMDTF	Geomagnetic Disturbance Task Force
GPS	Global positioning systems
HSPD-7	Homeland Security Presidential Directive 7
ISO PCS	Insurance Services Office Property Claims Services Division
IT	Information technology
LPTs	Large power transformers
Munich Re	Munich Reinsurance Company
MVA	Mega volt ampere
NAS	National Academy of Sciences
NERC	North American Electric Reliability Corporation
NFIP	National Flood Insurance Program
NOAA	National Oceanic and Atmospheric Administration
NSWP	U.S. National Space Weather Program
OE	Office of Electricity Delivery and Energy Reliability
OECD	Organisation for Economic Co-operation and Development
P.L.	Public Law
PPD-8	Presidential Policy Directive 8
PwC	PricewaterhouseCooper
SEC	U.S. Security and Exchange Commission
Swiss Re	Swiss Reinsurance Company Ltd.
TRIA	Terrorism Risk Insurance Act
UNISDR	United Nation Office for Disaster Reduction
US-CERT	U.S. Computer Emergency Readiness Team

Appendix B. Great and Devastating Natural Catastrophes Worldwide

Source: Munich Re, 2012.

Figure B1. Number of Great and Devastating Natural Catastrophes Worldwide From 1980 to 2010

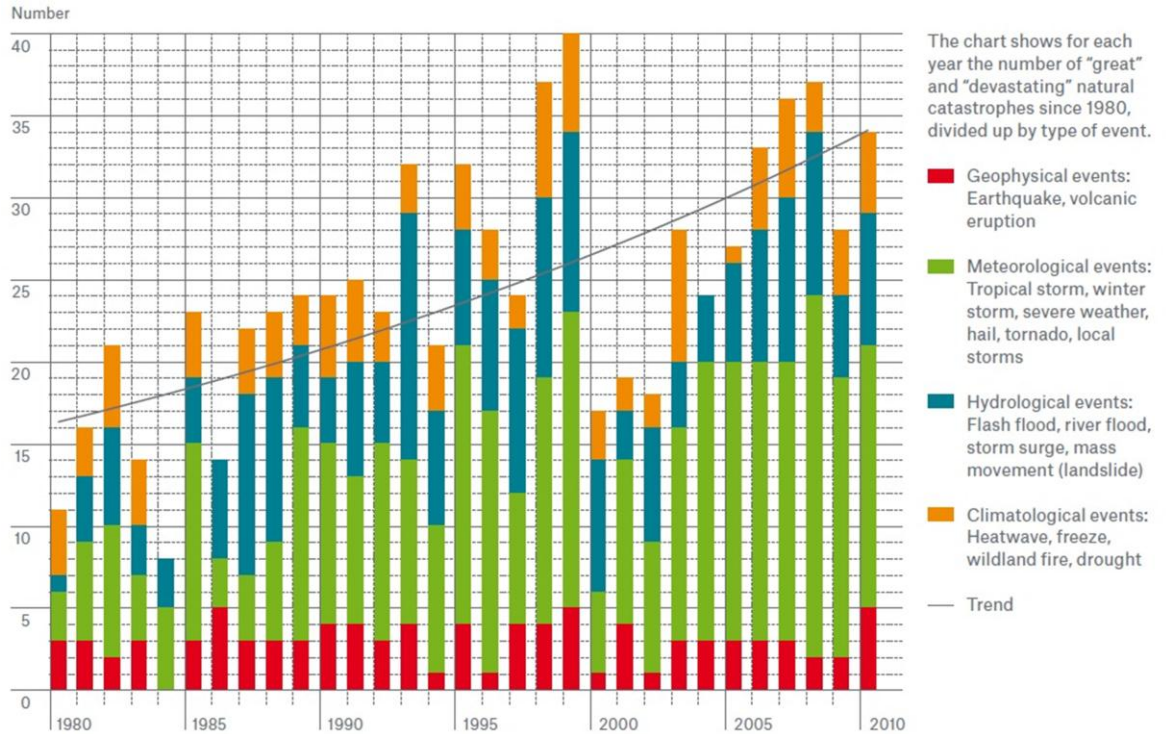
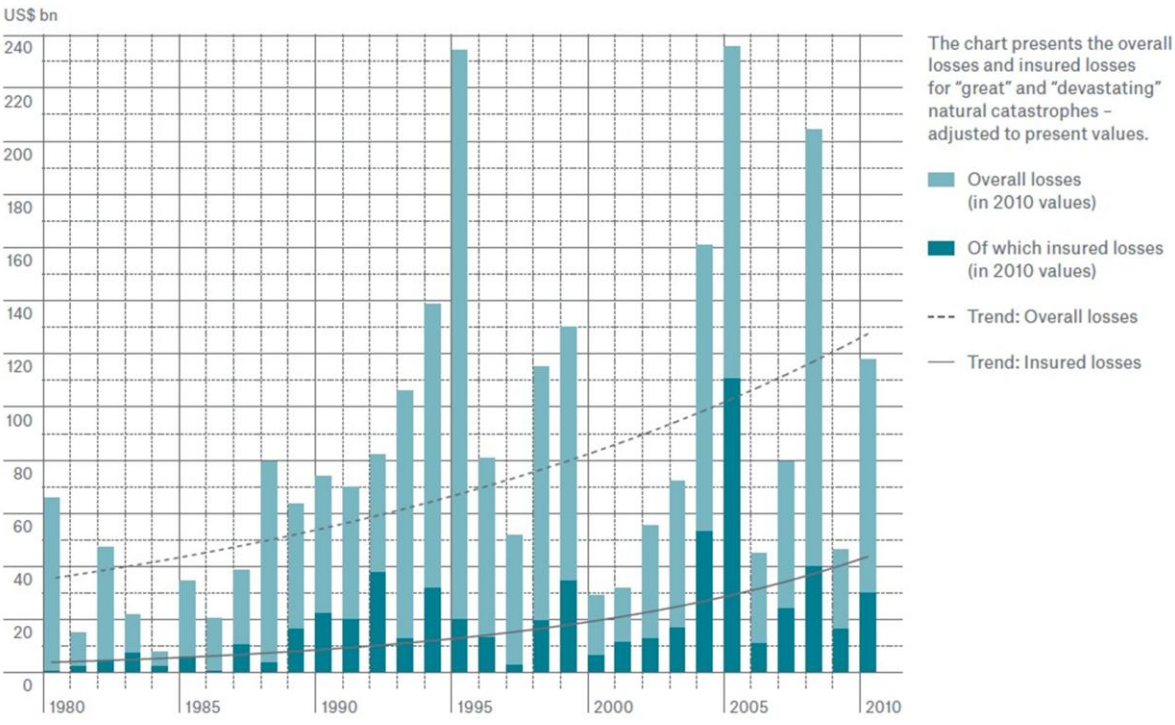


Figure B2. Losses From Great and Devastating Natural Catastrophes Worldwide From 1980 to 2010



Appendix C. Swiss Re's Assessment of Global Catastrophic Events

Source: Swiss Re Economic Research & Consulting, 2012.

Figure C1. Swiss Re's Assessment of Catastrophic Events Worldwide From 1980 to 2011

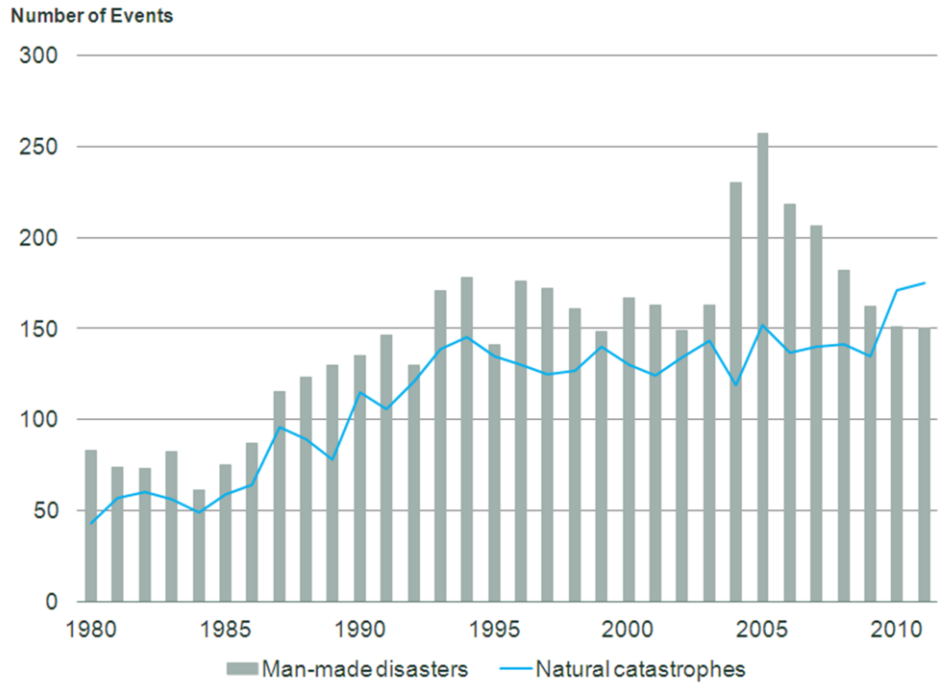
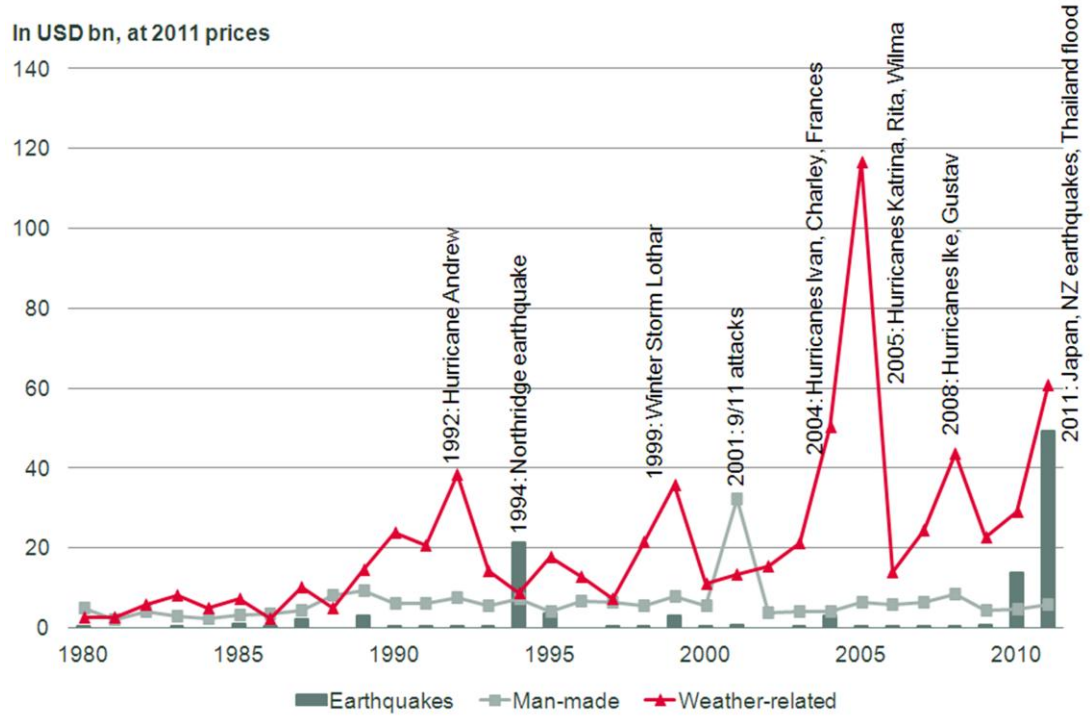


Figure C2. Insured Catastrophe Losses Worldwide From 1970 to 2011



Appendix D. Historical Natural Disaster Trends in the United States

Source: Munich Re, 2012.

Figure D1. U.S. Winter Storm Losses From 1900 to 2011 (Annual Totals)

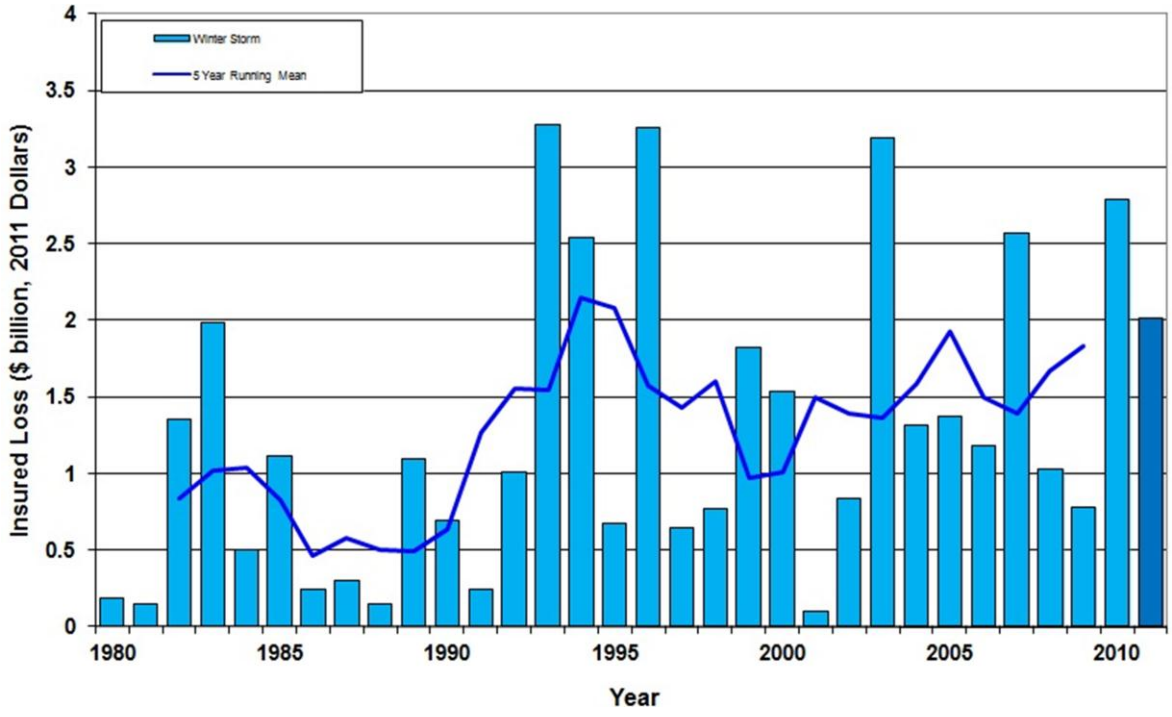


Figure D2. Number of U.S. Landfalling Tropical Cyclones From 1900 to 2011

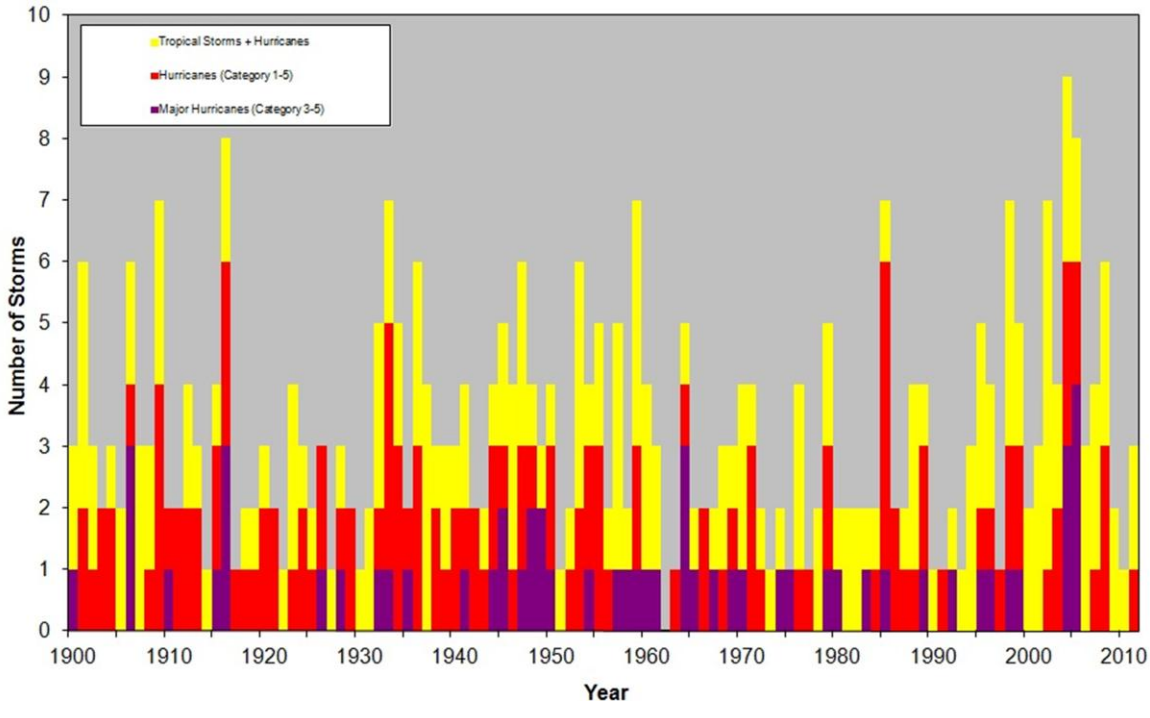


Figure D3. Insured U.S. Tropical Cyclone Losses From 1900 to 2011

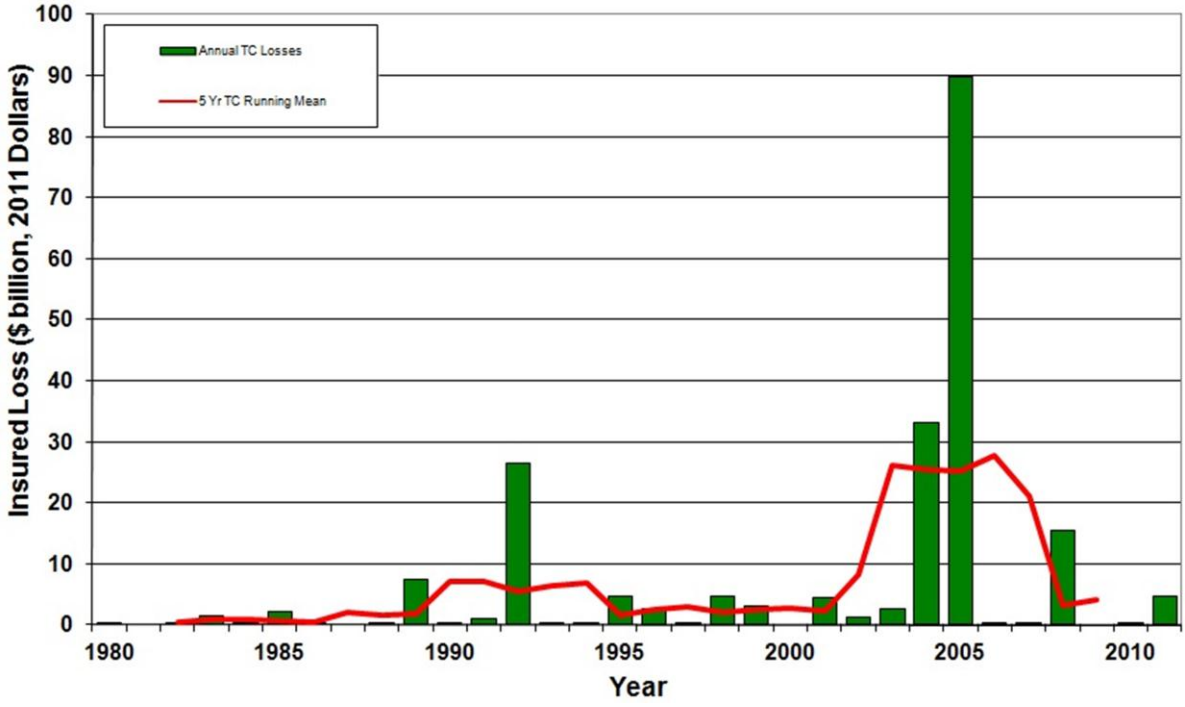
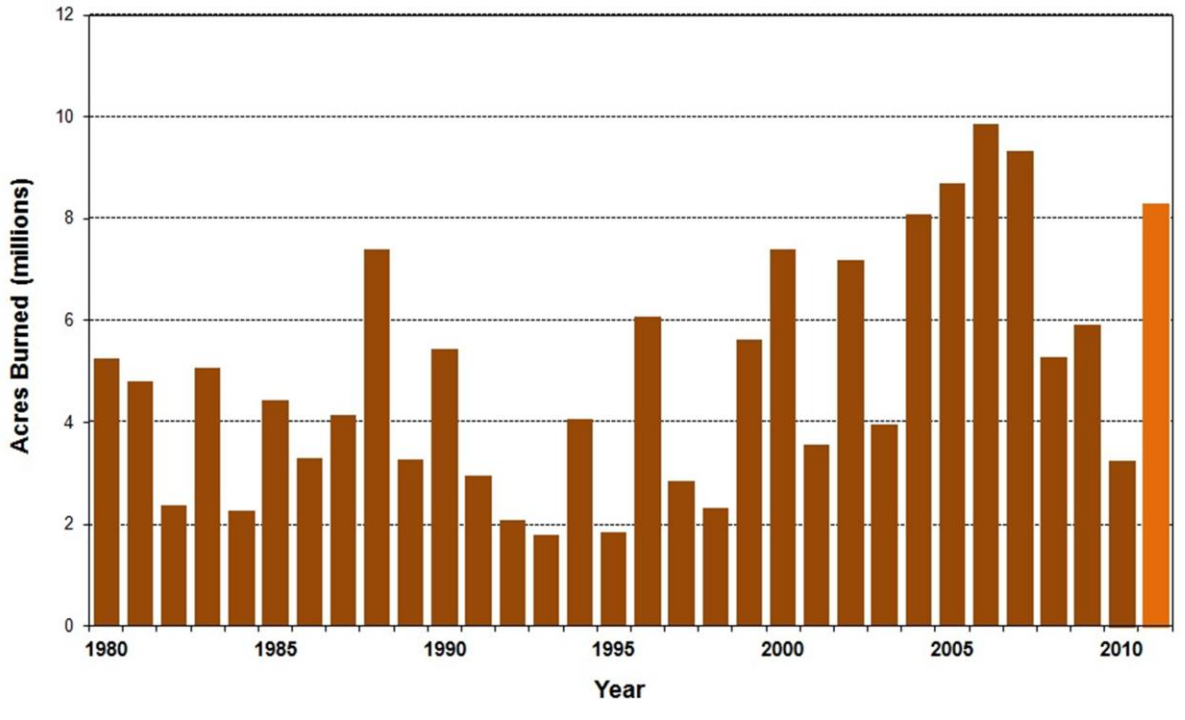


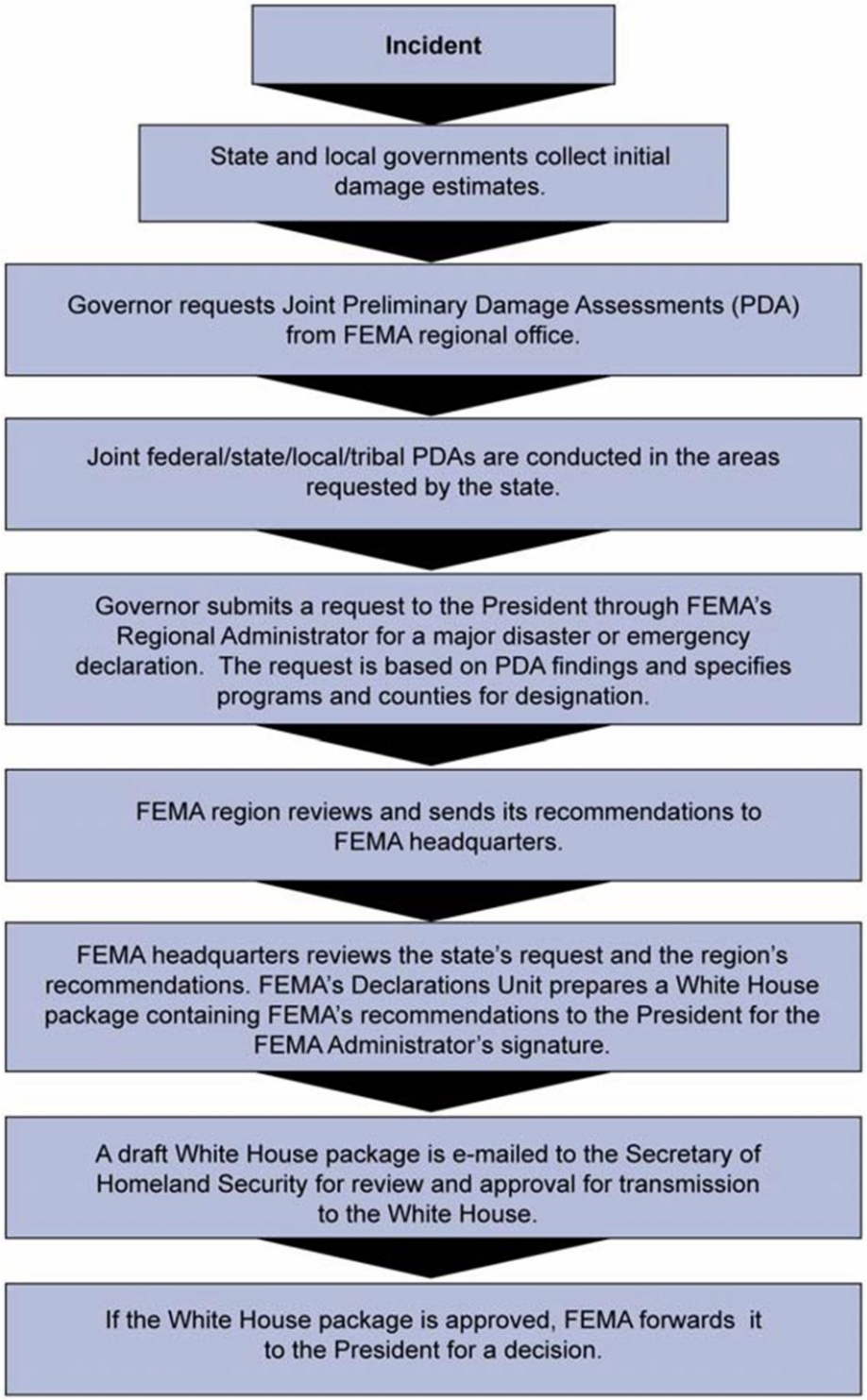
Figure D4. Number of Acres Burned in Wildfires From 1980 to 2011



Appendix E. Federal Emergency Declaration Process

Source: GAO, Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own, GAO-12-838, September 2012.

Figure E. Federal Emergency Declaration Process



Appendix F. Federal Insurance Programs

Source: GAO, Climate Change: Financial Risks to Federal and Private Insurers in Coming Decades Are Potentially Significant, GAO-07-285, March 2007.

Figure F1. National Flood Insurance Program Policies and Total Coverage

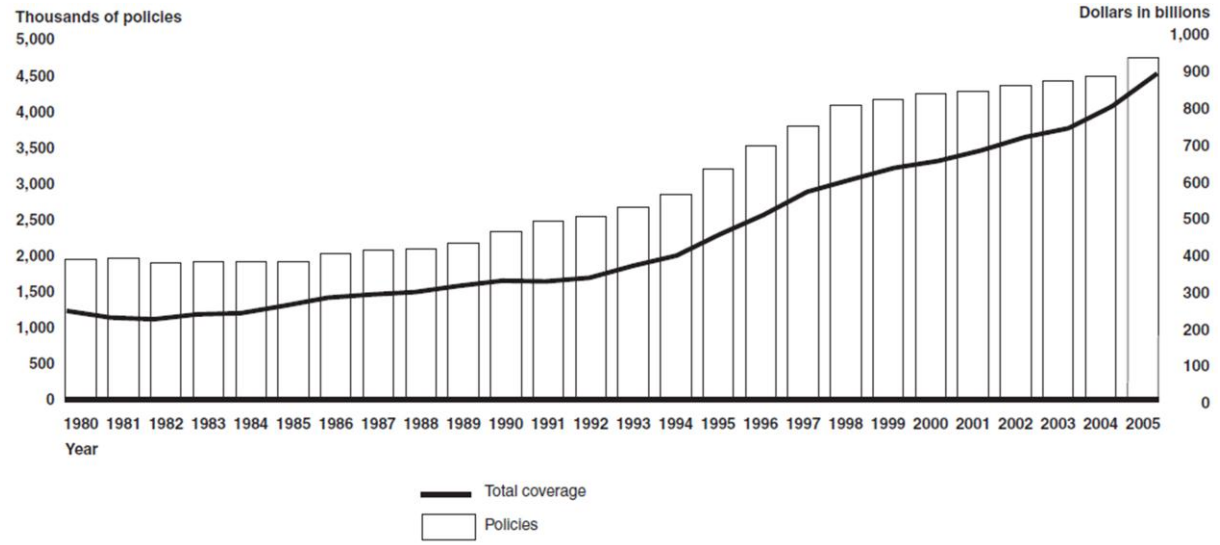


Figure F2. Weather-Related Losses Paid by the National Flood Insurance Program

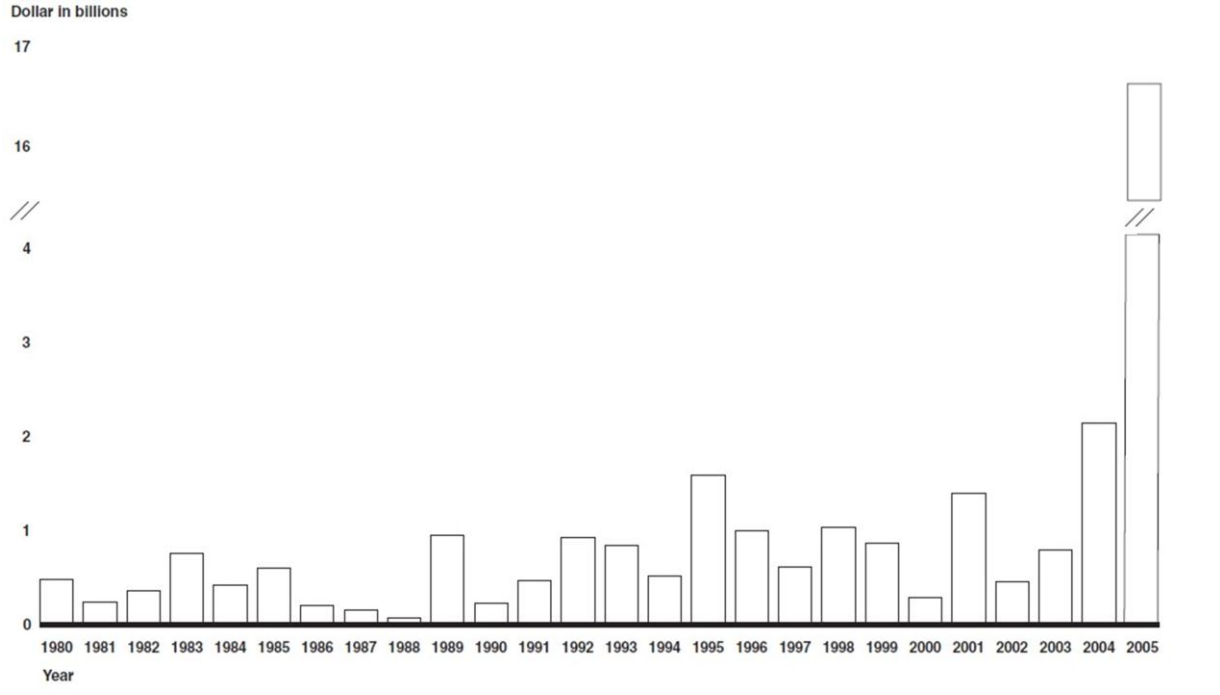


Figure F3. Federal Crop Insurance Corporation Total Coverage

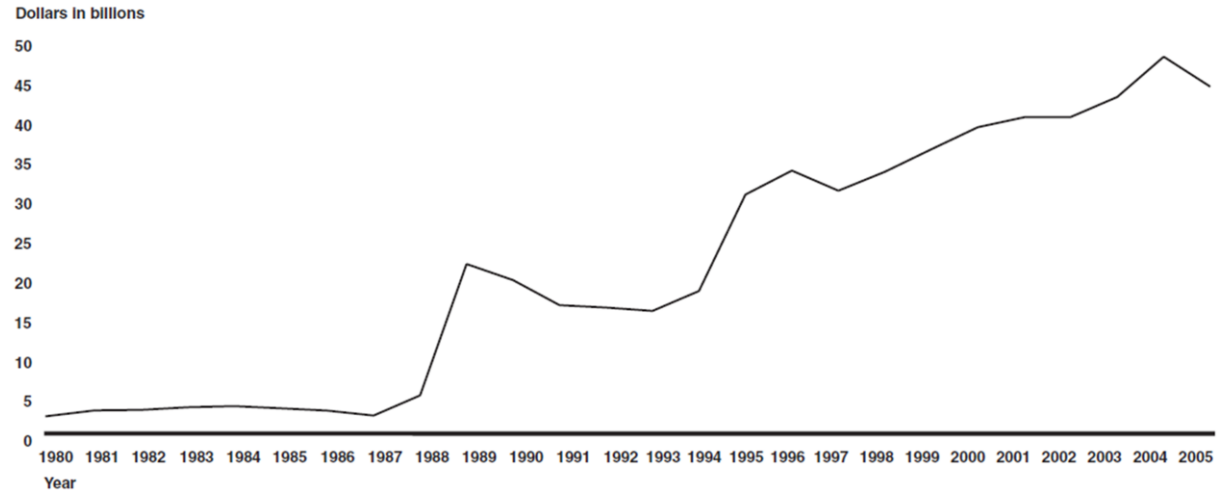
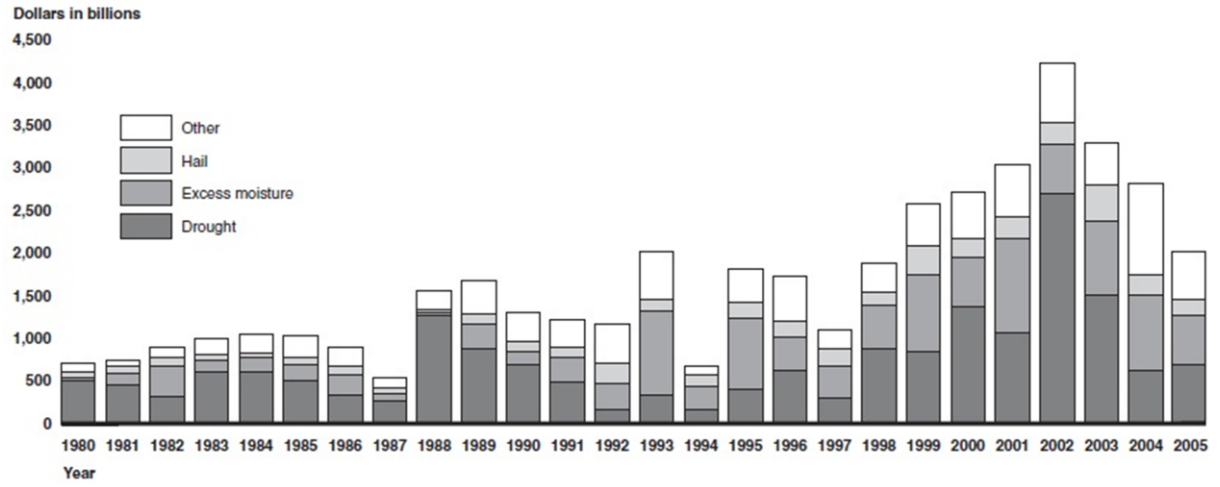


Figure F4. Weather-Related Losses Paid by the Federal Crop Insurance



Appendix G. Listing of All Accounts with Federal Insurance Activity

Source: GAO, Catalogue of Federal Insurance Activities, GAO-05-265R. March 4, 2005.

Administrative Office of the U.S. Courts
Judicial Officers' Retirement Fund
Judicial Survivors' Annuities Fund
United States Court of Federal Claims Judges' Retirement Fund
U.S. Agency for International Development
Development Credit Authority Guaranteed Loan Accounts
Housing and Other Credit Guaranty Programs
Loan Guarantees to Israel Accounts
Microenterprise and Small Enterprise Development Guaranteed Loans
Operating Expenses of the Agency for International Development (self-insurance)
Urban and Environmental Credit Program Guaranteed Loans
U.S. Central Intelligence Agency
Central Intelligence Agency Retirement and Disability System Fund
Export-Import Bank of the United States
Export-Import Bank Guaranteed Loan Accounts
Federal Council on the Arts and Humanities
National Endowment for the Arts (Arts and Artifacts Indemnity Program)
Federal Deposit Insurance Corporation
Bank Insurance Fund
FSLIC Resolution Fund
Savings Association Insurance Fund
International Security Assistance
Foreign Military Loan Liquidating Account
International Security Assistance Economic Support Fund
National Credit Union Administration
National Credit Union Share Insurance Fund
U.S. Office of Personnel Management
Civil Service Retirement and Disability Fund
Employees and Retired Employees Health Benefit Funds
Overseas Private Investment Corporation
Overseas Private Investment Corporation Guaranteed Loan Accounts
Overseas Private Investment Corporation Noncredit Account
Presidio Trust
Presidio Trust Fund
Presidio Trust Guaranteed Loan Accounts
U.S. Railroad Retirement Board
Railroad Industry Pension Fund
Railroad Unemployment Insurance Trust Fund
U.S. Securities and Exchange Commission
Securities and Exchange Commission, Salaries and Expenses (self-insurance)
U.S. Small Business Administration
Business Guaranteed Loan Accounts
Business Loan Fund Liquidating Account
Disaster Loan Fund Liquidating Account
Pollution Control Equipment Fund
Surety Bond Guarantees Revolving Fund
U.S. Social Security Administration
Federal Disability Insurance Trust Fund
Federal Old Age and Survivors Insurance (Social Security)
Social Security Administration, Limitation on Administrative Expenses (self-insurance)

Special Benefits for Certain World War II Veterans
U.S. Department of Agriculture
Agricultural Credit Insurance Fund Guaranteed Loan Accounts
Agricultural Credit Insurance Program Account (Dairy Indemnity Program)
Agricultural Resource Conservation Demonstration Guaranteed Loan Accounts
Animal and Plant Health Inspection Service (disease control compensation)
Capital Improvement and Maintenance (self-insurance)
Commodity Credit Corporation Export Guaranteed Loan Accounts
Farm Service Agency Salaries and Expenses (Non-Insured Crop Disaster Assistance Program)
Federal Crop Insurance Corporation Fund
Local Television Loan Guarantee Accounts
National Forest System (self-insurance)
Rural Business and Industry Guaranteed Loan Accounts
Rural Business Investment Program Guarantee Accounts
Rural Communication Development Fund Liquidating Account
Rural Community Advancement Program
Rural Community Facility Guaranteed Loan Accounts
Rural Development Insurance Fund Liquidating Account
Rural Electrification and Telecommunication Guaranteed Loan Accounts
Rural Housing Insurance Fund Guaranteed Loan Accounts
Rural Water and Waste Disposal Guaranteed Loan Accounts
Wildland Fire Management (self-insurance)
U.S. Department of Commerce
Economic Development Revolving Fund Liquidating Account
Emergency Oil and Gas Guaranteed Loan Accounts
Emergency Steel Guaranteed Loan Accounts
Federal Ship Financing Fund Fishing Vessels Liquidating Account
Fisheries Finance Guaranteed Loan Accounts
Fishermen's Contingency Fund
U.S. Department of Defense
Arms Initiative Guaranteed Loan Account
Defense Export Loan Guarantee Accounts
Family Housing Improvement Guaranteed Loan Accounts
Homeowners Assistance Fund
Military Personnel, Air Force (death gratuity)
Military Personnel, Army (death gratuity)
Military Personnel, Marine Corps (death gratuity)
Military Personnel, Navy (death gratuity)
Military Retirement Fund
National Guard Personnel, Air Force (death gratuity)
National Guard Personnel, Army (death gratuity)
Reserve Personnel, Air Force (death gratuity)
Reserve Personnel, Army (death gratuity)
Reserve Personnel, Marine Corps (death gratuity)
Reserve Personnel, Navy (death gratuity)
Revolving Fund (self-insurance)
Uniformed Services Retiree Health Care Fund
U.S. Department of Education
Federal Family Education Loan Accounts
Federal Student Loan Reserve Fund
U.S. Department of Health and Human Services
Federal Hospital Insurance Trust Fund (Medicare Part A)
Federal Supplementary Medical Insurance Trust Fund (Medicare Part B)
Food and Drug Administration, Salaries and Expenses (self-insurance)
Health Center Guaranteed Loan Accounts

Health Education Assistance Loan Accounts Health Maintenance Organization Loan and Loan Guarantee Fund Health Resources and Services General and Special Funds (Medical Malpractice Claims Fund) Medical Facilities Guarantee and Loan Fund Payments to Health Care Trust Funds Public Health and Social Services Emergency Fund (Smallpox Injury Compensation) Retirement Pay and Medical Benefits for Commissioned Officers (Public Health Service) State Children's Health Insurance Fund Substance Abuse and Mental Health Services Administration (self-insurance) Transitional Drug Assistance, Federal Supplementary Medical Assistance Trust Fund Vaccine Injury Compensation Vaccine Injury Compensation Program Trust Fund
U.S. Department of Homeland Security Customs and Border Protection (self-insurance) Citizenship and Immigration Services (self-insurance) Federal Protective Service (self-insurance) National Flood Insurance Fund Oil Spill Liability Trust Fund United States Coast Guard Operating Expenses (self-insurance) Retired Pay (U.S. Coast Guard)
U.S. Department of Housing and Urban Development Community Development Loan Guarantees Accounts FHA General and Special Risk Guaranteed Loan Accounts FHA General and Special Risk Insurance Funds Liquidating Account FHA-Loan Guarantee Recovery Fund Accounts FHA Mutual Mortgage and Cooperative Housing Insurance Funds Liquidating Account FHA Mutual Mortgage Insurance Guaranteed Loan Accounts Indian Federal Guarantees Accounts Indian Housing Loan Guarantee Fund Accounts Low-Rent Public Housing—Loans Native Hawaiian Housing Loan Guarantee Fund
U.S. Department of the Interior Indian Guaranteed Loan Accounts Indian Loan Guaranty and Insurance Fund Liquidating Account Natural Resource and Damage Assessment Fund (self-insurance) Resource Management (self-insurance)
U.S. Department of Justice Drug Enforcement Administration, Salaries and Expenses (self-insurance) Federal Prison System (self-insurance) Public Safety Officers' Benefits
U.S. Department of Labor Black Lung Disability Trust Fund Energy Employees Occupational Illness Compensation Fund Pension Benefit Guaranty Corporation Fund—Multi- and Single-Employer Program Special Benefits (Federal Employees) Special Benefits for Disabled Coal Miners Special Workers' Compensation Expenses Unemployment Trust Fund
U.S. Department of State Fishermen's Guaranty Fund Fishermen's Protective Fund Foreign Service Retirement and Disability Fund
U.S. Department of Transportation Aviation Insurance Revolving Fund Federal Ship Financing Fund Liquidating Account

Maritime Guaranteed Loan Title XI Accounts Minority Business Resource Center Guaranteed Loan Accounts Vessel Operations Revolving Fund (self-insurance) War Risk Insurance Revolving Fund (maritime)
U.S. Department of the Treasury Air Transportation Stabilization Guaranteed Loan Accounts Check Forgery Insurance Fund Claims, Judgments, and Relief Acts (Judgment Fund, self-insurance) District of Columbia Federal Pension Liability Trust Fund (and Federal Supplemental District of Columbia Fund) District of Columbia Judicial Retirement and Survivors Annuity Fund Processing, Assistance, and Management (self-insurance) Tax Law Enforcement (self-insurance) Payment of Government Losses in Shipment (self-insurance) Terrorism Insurance Program
U.S. Department of Veterans Affairs Burial Benefits (Veterans) Disability Compensation Benefits (Veterans) Housing Guaranteed Loan Accounts (Veterans) Insurance Benefits (Veterans Mortgage Life Insurance) National Service Life Insurance Fund (Veterans) Pension Benefits (Veterans) Service-Disabled Veterans Insurance Fund United States Government Life Insurance Fund (Veterans) Veterans Reopened Insurance Fund Veterans Special Life Insurance Fund
U.S. Postal Service Postal Service Fund (Domestic and Foreign Mail Indemnity Claim Fund)

Appendix H. Hurricane Damages to Oil and Natural Gas Infrastructure

Source: National Wildlife Federation, 2011.

SEVERE WEATHER	IMPACTS ON OIL AND GAS INFRASTRUCTURE
Wind	■ Toppled processing units or storage facilities ■ Dislodged roofs on refinery structures ■ Damaged piping and connections between storage and process units ■ Power failure or short circuiting, leading to the failure of steam boilers and cooling water towers ■ Damaged equipment, pipes, and tank roofs from projectiles, such as tree branches, signs, and rooftops ■ Pipelines damaged by dislocation of risers or host platform
Flooding	■ Short circuiting or power failure of electrical equipment (e.g., electrical lines, pumps), causing shut down of steam boilers, cooling towers, pumps, and electrically operated safety control mechanisms ■ Hazardous material releases from flooded internal plant drainage systems, compromised containment dikes, storage units damaged by storm surge, or torn pipe connections ■ Floating tank roofs can sink or tip, exposing oil on tank tops, vulnerable to fires in the case of lightning
Waves and subsea mudslides	■ Strong surface winds and currents can create significant underwater forces that damage pipelines[74] ■ Subsea mudslides, initiated by destabilization of shallow water areas in the Mississippi River delta, can destroy compressor platforms[75]
Lightning	■ Ignition of spilled oil could cause a fire or explosion

Appendix I. Summary Findings of Energy Hardening and Resilience Activities

Source: DOE/OE, "Hardening and Resilience: U.S. Energy Industry Response to Recent Hurricane Season," 2010.

		Industry Activities	Refineries/ Pipelines	Electric T&D
Hardening	Flood Protection	Building/strengthening berms, levees, and floodwalls	✓	
		Elevating substations/control rooms/pump stations	✓	✓
		Relocating/constructing new lines and facilities	✓	✓
	Wind Protection	Securing cooling towers	✓	
		Improving tank integrity	✓	
		Protecting cabling	✓	
		Protecting retail outlets	✓	
		Upgrading damaged poles and structures		✓
		Strengthening poles with guy wires		✓
		Burying power lines underground		✓
	Modernization	Upgrading electrical systems	✓	
		Installing/utilizing cogeneration	✓	
		Enhancing IT and telecommunications	✓	
		Deploying sensors and control technology		✓
		Installing asset databases/tools	✓	✓
Resiliency	General Readiness	Conducting hurricane preparedness planning and training	✓	✓
		Complying with inspection protocols	✓	✓
		Managing vegetation		✓
		Participating in mutual assistance groups		✓
		Improving employee communications and tracking	✓	
		Installing redundant communications	✓	
		Procuring mobile command vehicles	✓	
		Purchasing/leasing portable generators	✓	
		Pre-positioning and pre-wiring portable generators	✓	
		Securing alternate sources of gas supplies	✓	
		Purchasing or leasing mobile transformers and substations		✓
		Procuring spare T&D equipment		✓
	Storm-Specific Readiness	Maintaining minimum tank volumes	✓	
		Wrapping/protecting pumps and motors	✓	
		Facilitating employee evacuation and reentry	✓	✓
		Coordinating priority restoration and waivers	✓	
		Securing emergency fuel contracts		✓
		Supplying logistics to staging areas		✓

Appendix J. Bibliography

Allianz. (2011, November). "Blackout Risks." Retrieved August 19, 2012 from http://www.agcs.allianz.com/assets/PDFs/Special%20and%20stand-alone%20articles/Power_Blackout_Risks.pdf.

Allianz. (2012, April). "Emerging Risks 2012." Retrieved September 13, 2012 from http://www.agcs.allianz.com/assets/Global%20offices%20assets/UK/Documents/EMERGING%20RISKS%20REPORT%202012_low%20res.pdf.

Allianz. (2012, August). "Space Risks: A new generation of challenges." Retrieved November 27, 2012 from http://www.agcs.allianz.com/assets/PDFs/white%20papers/1844%20Allianz%20Space%20White%20Paper%201o.pdf.

American Geoscience Institute. "U.S. Vulnerability to Natural Hazards." Retrieved September 2, 2012 from http://www.agiweb.org/gap/workgroup/USHazPoster.pdf.

Auerswald, P., et. al. (2005, October). "The Challenge of Protecting Critical Infrastructure." Center for Risk Management and Decision Processes – The Wharton School of the University of Pennsylvania. Retrieved November 6, 2012 from http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf.

BestWire Services. (2011, March 28). "Japan Disaster Highlights the Need for Supply Chain Insurance." Retrieved August 19, 2012 from http://fpn.advisen.com/articles/article140935191888258975.html.

Bloomberg. (2012, February 1). "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months." Retrieved August 14, 2012 from, http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

Canadian Centre of Intelligence and Security Studies, the Norman Paterson School of International Affairs Carleton University. (2006, March). "Insurance and Critical Infrastructure Protection: Is there a Connection in an Environment of Terrorism?" Retrieved July 6, 2012 from http://www3.carleton.ca/cciss/res_docs/ceip/rowlands_devlin.pdf.

Ceres. (2012, May). "Physical Risks from Climate Change: A guide for companies and investors on disclosure and management of climate impacts." Retrieved June 27, 2012 from http://www.ceres.org/resources/reports/physical-risks-from-climate-change.

Claverol, M. (2012, September 23). "Space Weather- The Peril of The Future? Understanding Business Interruption Claims." Property Insurance Coverage Law Blog. Retrieved October 31, 2012 from http://www.propertyinsurancecoveragelaw.com/2012/09/articles/commercial-insurance-claims/space-weather-the-peril-of-the-future-understanding-business-interruption-claims/.

Commercial Risk Europe. Retrieved October 17, 2012 from http://www.commercialriskeurope.com/.

Commercial Risk Europe. (2011). "Risk Frontier Survey 2011." Retrieved October 18, 2012 from http://www.commercialriskeurope.com/uploads/files/special-reports/Risk-Frontiers-Survey-2011.pdf.

Cox, J. (2012, November 19). "Sandy's Impact on Job Growth Will Be 'Acute': LaVorgna." CNBC. Retrieved November 19, 2012 from http://www.cnbc.com/id/49883615.

CRO Forum. Retrieved October 2, 2012 from http://www.thecroforum.org/about.html.

CRO Forum. (2008, November). "Critical Information Infrastructure: The digital economy's Achilles heel." Retrieved July 18, 2012 from http://www.thecroforum.org/assets/files/publications/CRO%20Position%20Paper%20-%20Critical%20Information%20Infrastructure.pdf.

CRO Forum. (2011, November). "Power Blackout Risks: Risk Management Options." Retrieved November 1, 2012 from http://www.thecroforum.org/assets/files/publications/CRO-Position%20Paper%20-%20Power%20Blackout%20Risks-.pdf.

CRO Forum. "Emerging Risk Initiative." Retrieved September 13, 2012 from http://www.thecroforum.org/emerging_risks_initiative.html.

DHS (U.S. Department of Homeland Security). (2011, March 11). Presidential Policy Directive / PPD-8: National Preparedness. Retrieved June 29, 2012 from http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

DHS. (2011, May). "Risk Management Issue Brief: Geomagnetic Storms: An Evaluation of Risks and Risk Assessments." Retrieved August 16, 2012 from http://www.dhs.gov/xlibrary/assets/rma-geomagnetic-storms.pdf.

DOE (U.S. Department of Energy). (2010, August). "Hardening and Resilience: U.S. Energy Industry Response to Recent Hurricane Season." Retrieved August 23, 2012 from http://www.oe.netl.doe.gov/docs/HR-Report-final-081710.pdf.

DOE. (2012, June). "Large Power Transformers and the U.S. Electric Grid." Retrieved October 30, 2012 from http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

DOE. Emergency Support Function #12 – Energy Annex. Retrieved November 1, 2012 from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf.

E&E News. (2012, July 12). "State insurance programs continue to grow amid hurricane lull." Retrieved August 15, 2012 from http://eenews.net/public/climatewire/2012/07/12/1.

DHS and DOE. (2010). The Energy Sector Specific Plan. Retrieved June 29, 2012 from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_2010.pdf.

DHS and DOE. (2011, September). "Dams and Energy Sectors Interdependency Study." Retrieved November 7, 2012 from http://energy.gov/sites/prod/files/Dams-Energy%20Interdependency%20Study.pdf.

Edison Electric Institute. (2005, February). "After the Disaster: Utility Restoration Cost Recovery." Retrieved August 21, 2012 from http://www.eei.org/ourissues/electricitydistribution/Documents/Utility_Restoration_Cost_Recovery.pdf.

Entergy Corporation. (2010). "Building a Resilient Gulf Coast: Executive Report." Retrieved August 20, 2012 from http://www.entergy.com/content/our_community/environment/GulfCoastAdaptation/Building_a_Resilient_Gulf_Coast.pdf.

European Network and Information Security Agency. (2012, June). "Incentives and barriers of the cyber insurance market in Europe." Retrieved September 13, 2012 from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport.

Federal Register. (2012, October 24). "Reliability Standards for Geomagnetic Disturbances." Notice of Proposed Rulemaking, Docket No. RM12-22-000. Retrieved October 24, 2012 from https://www.federalregister.gov/articles/2012/10/24/2012-26131/reliability-standards-for-geomagnetic-disturbances.

FEMA (Federal Emergency Management Agency). Declared Disasters by Year or State. Retrieved June 28, 2012 from http://www.fema.gov/news/disaster_totals_annual.fema.

FEMA. Disaster Declaration Process. Retrieved June 1, 2012 from http://www.fema.gov/media/fact_sheets/declaration_process.shtm.

FEMA. Training Course, "Comparative Emergency Management: Session 16: Risk Transfer, Sharing, and Spreading."

GAO. (2005, March 4). Catalogue of Federal Insurance Activities, GAO-05-265R. Retrieved September 24, 2012 from http://www.gao.gov/assets/100/93046.pdf.

GAO. (2005, July 28). Ultimate Effects of McCarran-Ferguson Federal Antitrust Exemption on Insurer Activity Are Unclear, GAO-05-816R. Retrieved November 27, 2012 from http://www.gao.gov/new.items/d05816r.pdf.

GAO. (2006, February 23). Definitions of Insurance and Related Information, GAO-06-424R. Retrieved June 29, 2012 from http://www.gao.gov/assets/100/94044.pdf.

GAO. (2007, November). Natural Disasters: Public Policy Options for Changing the Federal Role in Natural Catastrophe Insurance, GAO-08-7. Retrieved July 23, 2012 from http://www.gao.gov/new.items/d087.pdf.

GAO. (2012, April 24, 2012). Cybersecurity: Threats Impacting the Nation, GAO-12-666T. Retrieved August 10, 2012 from http://www.gao.gov/assets/600/590367.pdf.

GAO. (2012, September). Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own, GAO-12-838. Retrieved November 19, 2012 from http://www.gao.gov/assets/650/648162.pdf.

Geneva Association. (2011). "Global insurance industry fact-sheet." Retrieved July 5, 2012 from http://www.genevaassociation.org/pdf/News/2011globalinsuranceindustryfactsheet.pdf.

Geneva Association. (2012, March). "Extreme events and insurance: 2011 annus horribilis." Retrieved July 5, 2012 from http://www.genevaassociation.org/PDF/Geneva_Reports/GA-2012-Geneva_report%5B5%5D.pdf.

Gould, A.J., Linden, O.M. (2000). "Estimating Satellite Insurance Liabilities." Casualty Actuarial Society. Retrieved November 5, 2012 from http://www.casact.org/pubs/forum/00fforum/00ff047.pdf.

Grannis, J. (2012, August 14). "Analysis of How the Flood Insurance Reform Act of 2012 (H.R. 4348) May Affect State and Local Adaptation Efforts." Georgetown Climate Center. Retrieved August 16, 2012 from http://www.georgetownclimate.org/sites/default/files/Analysis%20of%20the%20Flood%20Insurance%20Reform%20Act%20of%202012.pdf.

Hartwig, R.P., Ph.D. (2012, September 11). Testimony of Robert P., Ph.D., CPCU, President & Economist, Insurance Information Institute, before the House Committee on Financial Services, Subcommittee on Insurance, Housing and Community Opportunity, "TRIA at Ten Years: The Future of the Terrorism Risk Insurance Program." Washington, D.C. Retrieved October 30, 2012 from http://financialservices.house.gov/uploadedfiles/hhrg-112-ba04-wstate-rhartwig-20120911.pdf.

Harrison, J.D. (2011, December 28). "Cybersecurity insurance: What small businesses need to know." *Washington Post.* Retrieved October 8, 2012 from http://www.washingtonpost.com/blogs/on-small-business/post/cybersecurity-insurance-what-small-businesses-need-to-know/2011/12/28/gIQAYlL5MP_blog.html.

Hemenway, C. (2012, August 10). "Chubb Survey: Concern of Cyber Risk Not Leading to Insurance Buy." Property Casualty 360. Retrieved September 18, 2012 from http://www.propertycasualty360.com/2012/08/10/chubb-survey-concern-of-cyber-risk-not-leading-to.

Hernandez, R. (2013, January 4). "Congress Passes a $9.7 Billion Storm Relief Measure." *New York Times.* Retrieved February 7, 2013 from http://www.nytimes.com/2013/01/05/nyregion/house-passes-9-7-billion-in-relief-for-hurricane-sandy-victims.html.

Holm, E. (2012, November 14). "Sandy May Cost Insurers Up to $25 Billion." *Wall Street Journal.* Retrieved November 19, 2012 from http://online.wsj.com/article/SB10001424127887324735104578119301366617508.html.

Insurance Information Institute. Glossary. Retrieved July 3, 2012 from http://www2.iii.org/glossary/index.cfm.

Insurance Information Institute. "Inflation Adjusted U.S. Catastrophe Losses by Causes of Losses from 1991 to 2011." Retrieved August 23, 2012 http://www.iii.org/index.cfm?instanceID=242789.

Insurance Information Institute. "What Does a Businessowners Policy (BOP) Cover?" Retrieved October 23, 2012 from http://www.iii.org/articles/what-does-a-businessowners-policy-cover.html.

Internet Security Alliance. "Cyber-Insurance Metrics and Impact on Cyber-Security." Retrieved September 19, 2012 from http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

Insurance Services Office Property Claims Services Division (ISO PCS). "PCS Catastrophe Serial Numbers." Retrieved February 7, 2013 from http://www.iso.com/Products/Property-Claim-Services/PCS-Catastrophe-Serial-Numbers.html

Kappenman, John G., et al. (1990). "Solar Wind Monitor Satellite Crucial for Geomagnetic Storm Warning." *IEEC Power Engineering Review.*

King, R. P. (2011, July 1). "National Flood Insurance Program: Background, Challenges, and Financial Status." *Congressional Research Services.* Retrieved August 9, 2012 from http://www.fas.org/sgp/crs/misc/R40650.pdf.

King, R. (2012, May 29). "As Flame Spreads, Most Companies Lack Cybersecurity Coverage." *Wall Street Journal.* Retrieved October 8, 2012 from http://blogs.wsj.com/cio/2012/05/29/as-flame-spreads-most-companies-lack-cybersecurity-coverage/.

Koebler, J. (2012, March 5). "Experts: Extreme Solar Storm Could Cause Cosmic 'Katrina'." *U.S. News.* Retrieved September 20, 2012 from http://www.usnews.com/news/articles/2012/03/05/experts-extreme-solar-storm-could-cause-cosmic-katrina.

Lawder, D. (2013, January 28). "Senate votes to approve $50.5 billion Sandy aid package." *Reuters.* Retrieved on February 7, 2013 from http://www.reuters.com/article/2013/01/28/us-usa-congress-sandy-idUSBRE90R10620130128.

Lawrence Berkeley National Laboratory. (2009, June). "Estimated Value of Service Reliability for Electric Utility Customers in the United States." Retrieved August 18, 2012 from http://certs.lbl.gov/pdf/lbnl-2132e.pdf.

Lloyd's. (2010). "Solar Weather: Its impact on Earth and implications for business." Retrieved September 21, 2012 from http://www.lloyds.com/~/media/Lloyds/Reports/360/360%20Space%20Weather/7311_Lloyds_360_Space%20Weather_03.pdf.

Lloyd's. (2010, November). "Space Weather: Its Impact on Earth and implications for business." Retrieved October 12, 2012 from http://www.lloyds.com/~/media/Lloyds/Reports/360/360%20Space%20Weather/7311_Lloyds_360_Space%20Weather_03.pdf.

Lloyd's. (2011). "Managing the escalating risks of natural catastrophes in the United States." Retrieved July 19, 2012 from http://www.lloyds.com/~/media/Lloyds/Reports/Emerging%20Risk%20Reports/Natural%20Catastrophes%20in%20the%20US.pdf.

Lloyd's. (2011, January 10). "Future Risks Take Shape in 2011." Retrieved August 23, 2012 from http://www.lloyds.com/News-and-Insight/News-and-Features/360-News/Business-360/Future-risks-take-shape-in-2011.

Lloyd's. (2011, December 15). "Emerging Risks Management at Lloyd's." Retrieved August 3, 2012 from http://www.theirm.org/events/documents/NSmithpresentation.pdf.

Marsh. (2011, April). "Cyber risks: Understanding your insurance protection." Retrieved September 19, 2012 from http://usa.marsh.com/Portals/9/Documents/UnderstandingCyberRisks2011.pdf.

Munich Re. (2005, November). "The Increasing Costs of Natural Disasters." *Geotimes,* The Princeton University. Retrieved July 23, 2012 from http://www.princeton.edu/geosciences/people/vandervink/pdf/harzardcostarticle-geotimes-lo.pdf.

Munich Re. (2011). "TOPICS GEO, Natural catastrophes 2010: Analyses, assessments, positions." Retrieved November 23, 2012 from www.munichre.com/publications/302-07225_en.pdf.

Munich Re. (2011, April 26). Eichner, J., "Space Weather Risks from an Insurance perspective." Retrieved October 31, 2012 from http://www.swpc.noaa.gov/sww/sww11/SWW_2011_Presentations/SWW_Boulder_MunichRE_EICHNER.pdf.

Munich Re. (2012, January 4). Press Release. Retrieved June 22, 2012 from http://www.munichre.com/en/media_relations/press_releases/2012/2012_01_04_press_release.aspx.

Munich Re. (2005). Hoeppe, P. "Worldwide Natural Disasters-Effects and Trends." Retrieved July 18, 2012 from http://www.munichre-foundation.org/NR/rdonlyres/E7ED6B1D-2D9F-4E64-9FB3-5C8A4539AD9B/0/20051116_Hoeppe_Hohenkammer_short_WEB.pdf.

Munich Re. Loss database for natural catastrophes worldwide. Retrieved July 6, 2012 from http://www.munichre.com/app_pages/www/@res/pdf/natcatservice/database/catastrophe_classes_touch_en.pdf.

Much Re. NatCatSERVICE. Retrieved August 29, 2012 from http://www.munichre.com/en/reinsurance/business/non-life/georisks/natcatservice/default.aspx.

"Munich Re: 2012 Natural Disasters Cost Global Insurers $65B Vs $119B." (2013, January 3). *Wall Street Journal.* Retrieved February 7, 2013 from http://online.wsj.com/article/BT-CO-20130103-701942.html.

National Academy of Sciences. (1999). "The Impacts of Natural Disasters: A Framework for Loss Estimation." Washington, D.C.

National Research Council of the National Academies. (2008). "Severe Space Weather Events—Understanding Societal and Economic Impacts, A Workshop Report." Retrieved October 31, 2012 from http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf.

National Wildlife Federation. (2011). "More Extreme Weather and the U.S. Energy Infrastructure." Retrieved June 29, 2012 from http://www.nwf.org/~/media/PDFs/Global-Warming/Extreme-Weather/Final_NWF_EnergyInfrastructureReport_4-8-11.ashx.

NERC (North American Electric Reliability Corporation). (2010, June). "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System." Retrieved March 25, 2013 from http://www.nerc.com/files/HILF.pdf.

NERC. (2012, February). "2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System." Retrieved September 20, 2012 from http://www.nerc.com/files/2012GMD.pdf.

NOAA (National Oceanic and Atmospheric Administration). (2004, September). "Population Trends Along the Coastal United States: 1980-2008." Retrieved June 28, 2012 from http://oceanservice.noaa.gov/programs/mb/pdfs/coastal_pop_trends_complete.pdf.

NOAA. Space Weather Prediction Center. Retrieved September 20, 2012 from http://www.swpc.noaa.gov/.

Nordman, E. C., National Association of Insurance Commissioners, 2010.

Nutter, F. (2012, December). Reinsurance Association of America, Presented December 14, 2012. Retrieved December 18, 2012 from http://files.eesi.org/121412_Frank_Nutter.pdf.

Odenwald, S. and Green, J. (2008, July 28). "Bracing the Satellite Infrastructure for a Solar Superstorm." *Scientific American.* Retrieved September 21, 2012 from http://www.scientificamerican.com/article.cfm?id=bracing-for-a-solar-superstorm&page=5.

Office of Management and Budget. (2012, March 7). "Fiscal Year 2011Report to Congress on the Implementation of The Federal Information Security Management Act of 2002." Retrieved September 28, 2012 from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf.

Organisation for Economic Co-operation and Development (OECD). (2012, June). Improving the Assessment of Disaster Risks to Strengthen Financial Resilience: A Special Joint G20 Publication by the Government of Mexico and the World Bank, Chapter 17 Annex - OECD: Review of the Main Initiatives on Collection and Dissemination of Cat Risk Exposures and Losses. Retrieved February 11, 2013 from http://www.gfdrr.org/sites/gfdrr.org/files/GFDRR_G20_Low_June13.pdf.

Palmer, M. (2011, November 1). "Insurance: The trade-off between risk and cost." *Financial Times*. Retrieved September 13, 2012 from http://www.ft.com/cms/s/0/9d4045a6-f8a1-11e0-ad8f-00144feab49a.html#axzz26NQoasuu.

Perlroth, N. (2011, December 23). "Insurance Against Cyber Attacks Expected to Boom." *New York Times.* Retrieved October 18, 2012 from http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/.

Ponemon Institute. (2011, April). "State of IT Security: Study of Utilities & Energy Companies." Retrieved September 19, 2012 from http://www.all-about-security.de/fileadmin/micropages/Krims_Krams_Pdfs/State-of-IT-Security--Study-of-Utilities-and-Energy-Companies.pdf.

Ponemon Institute. (2011, August). "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies." Sponsored by ArcSight, an HP Company. Retrieved October 24, 2012 from http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

PricewaterhouseCooper. The Global State of Information, Security Survey 2013. Retrieved October 23, 2012 from http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#.

Pub. L. No. 79-5, Ch. 20, 59 Stat. 33 (1945) codified as amended at 15 U.S.C. §§ 1011-1015.

Rice, D. (2012, November 16). "Sandy ends hurricane season on forceful note." *USA Today*. Retrieved November 16, 2012 from http://www.usatoday.com/story/weather/2012/11/15/sandy-brought-violent-end-to-hurricane-season/1707839/.

Riswadkar, A.V. and Dobbins, B. (2010, April 8). "Solar Storms: Protecting Your Operations Against the Sun's 'Dark Side'." Zurich Services Corporation. Retrieved September 20, 2012 from http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/media/solarstorms.pdf.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 U.S.C. 5121-5207, and Related Authorities. Retrieved May 31, 2012 from http://www.fema.gov/pdf/about/stafford_act.pdf.

Sagalow, Ty R. (2002). *The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce, and cyber perils*. Reactions Publishing Group, Ltd., London, United Kingdom.

Sclafane, S. (2012, March). "Advisen Spotlight: Emily Freeman on the Cutting Edge." *Advisen Cyber Liability Journal.* Retrieved October 15, 2012 from http://corner.advisen.com/pdf_files/CLJ_Q1_2012.pdf.

SEC (Securities and Exchange Commission). (2011, October 13). Division of Corporation Finance. "CF Disclosure Guidance: Topic No. 2—Cybersecurity." Retrieved October 18, 2012 from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Shields, D. A. (2010, December 13). "Federal Crop Insurance: Background and Issues." *Congressional Research Service.* Retrieved August 10, 2012 from http://www.nationalaglawcenter.org/assets/crs/R40532.pdf.

Strategic Risk. (2012, March). "Evolving cyber cover." Retrieved September 17, 2012 from http://www.strategic-risk.eu/Journals/2012/02/22/i/j/w/RiskFinancing_Mar12.pdf.

Swiss Re. (2000). "Space Weather, Hazard to the Earth?" Retrieved August 16, 2012 from http://media.swissre.com/documents/pub_space_weather_en.pdf.

Swiss Re. (2010). "The essential guide to reinsurance." Retrieved July 5, 2012 from http://media.swissre.com/documents/The_Essential_Guide_to_Reinsurance_EN.pdf.

Swiss Re. (2012, February). "Natural catastrophes and man-made disasters in 2011: historic losses surface from record earthquakes and floods." Sigma. Retrieved July 9, 2012 from http://media.swissre.com/documents/sigma2_2012_en.pdf.

Swiss Re. Insured catastrophe losses, 1970-2011. Sigma. Retrieved August 22, 2012 from http://www.swissre.com/sigma/.

Swiss Re. "Spotlight on emerging risks." Retrieved October 1, 2012 from http://www.swissre.com/rethinking/emerging_risks/QA_Reto_Schneider.html.

The Betterley Report. (2012, August). Cyber/Privacy Insurance Market Survey—2012: Surprisingly Competitive, as Carriers Seek Market Share. Retrieved September 17, 2012 from http://betterley.com/samples/cpims12_nt.pdf.

The Economist. (2012, January 14). "Natural disasters: Counting the cost of calamities." Retrieved July 18, 2012 from http://www.economist.com/node/21542755.

The Homeland Security Act of 2002, Public Law 109-295, as amended, 6 U.S.C. 311-321. Retrieved June 25, 2012 from http://uscode.house.gov/pdf/2006/2006usc06.pdf.

The Rocky Mountain Climate Organization. (2012, May). "Doubled Trouble: More Midwestern Extreme Storms." Retrieved June 28, 2012 from http://www.rockymountainclimate.org/images/DoubledTroubleHigh.pdf.

Towers Watson. (2012, April). "2012 Risk and Finance Manager Survey." Retrieved October 8, 2012 from http://www.towerswatson.com/assets/pdf/6842/2012-Risk-and-Finance-Manager-Survey-PDF.pdf.

United Nation Office for Disaster Reduction (UNISDR). (2009). UNISDR Terminology on Disaster Risk Reduction, Retrieved June 26, 2012 from http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf.

U.S. Census Bureau. (2010, May). "Coastline Population Trends in the United States: 1960 to 2008." Retrieved June 28, 2012 from http://www.census.gov/prod/2010pubs/p25-1139.pdf.

US-CERT (U.S. Computer Emergency Readiness Team). Retrieved August 10, 2012 from http://www.us-cert.gov/.

US-CERT. (2012, June). "ICS-CERT Incident Response Summary Report." Retrieved September 13, 2012 from http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf.

US-CERT. About US-CERT. Retrieved August 10, 2012 from http://www.us-cert.gov/about-us/.

World Economic Forum. Retrieved October 2, 2012 from http://www.weforum.org/.

World Economic Forum. (2011). Global Risks 2011, Sixth Edition. Retrieved November 27, 2012 from http://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf.

World Economic Forum. (2012). Global Risks 2012, Seventh Edition. Retrieved August 10, 2012 from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.